ЧЕК-ЛИСТ ДЛЯ CFO: РЕАГИРОВАНИЕ НА КИБЕРАТАКУ *и восстановление* РАБОТЫ КОМПАНИИ

Андрей Кузин

Операционный директор,
Positive Technologies

Алексей Лукацкий

Бизнес-консультант по информационной безопасности, Positive Technologies

Этот чек-лист — рабочий инструмент для CFO и финансово-операционной команды. Его можно использовать:

› как шпаргалку — что проверить и о чем не забыть на разных этапах (первые сутки после кибератаки, первые недели, 1–3 месяца спустя);

› как основу для регламента по внутреннему реагированию на киберинциденты;

› как чек-лист для ретроспективы — можно пройтись по нему после инцидента и понять, что было сделано, а что стоит добавить в будущем.

Не обязательно проходить чек-лист строго сверху вниз — в реальной жизни части будут идти параллельно. Главное, чтобы по итогам у CFO был честный ответ на вопросы: что мы сделали; что сознательно не делаем; где у нас дыры, которые нужно закрыть?

ЧТО *обычно* БОЛИТ У CFO ПОСЛЕ КИБЕРАТАКИ

В большинстве кейсов CFO сталкивается не с абстрактной кибератакой, а с очень приземленными последствиями:

› Остановка или резкое замедление ключевых бизнес-процессов — производства, логистики, отгрузок, биллинга, казначейства, продаж.

› Невозможность нормально проводить платежи (клиент-банк недоступен, банк видит нетипичные операции, повышается риск блокировок).

› Потеря или искажение учетных данных — бухгалтерских и налоговых регистров, данных по взаиморасчетам, кадровых данных, информации для расчета зарплаты.

› Риски по налогам и регуляторам — невозможность предоставить документы за 3 года, претензии ФНС, Роскомнадзора, СФР, налоговые и даже уголовные последствия.

› Финансовые потери — падение выручки, срыв контрактов, штрафы и неустойки, дополнительные расходы на восстановление и ручной труд.

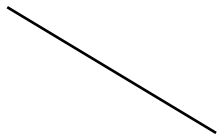
› Обострение отношений с внешними стейкхолдерами: банками (ковенанты, лимиты, «подозрительное поведение»), акционерами, советом директоров, крупными клиентами и партнерами.

› Риски для менеджмента — вопросы «Кто виноват?», попытки повесить ответственность на CFO/ИТ/ИБ/гендиректора, уголовные претензии.

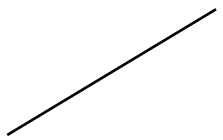
Дальше — пошаговый чек-лист, который поможет минимизировать эти последствия. Что делать в первые 24 часа → первые 72 часа → 2–4 недели → 1–3 месяца + советы по защите менеджмента и уроки на будущее.

ОБЩИЕ *принципы* ДЛЯ CFO

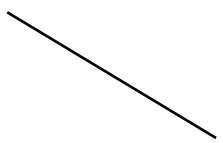
» Сначала — устойчивость компании и ликвидность, и уже потом — «красота» отчетности.



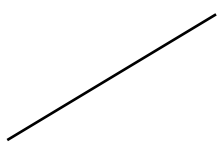
» Все ключевые решения должны быть в каком-то виде зафиксированы: служебные записки, письма, e-mail, мессенджеры с последующей легализацией.



» Лучше «переобъяснить» регуляторам, чем промолчать.

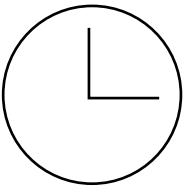


» CFO — связующее звено между акционерами, банками, регуляторами и ИТ/ИБ.



» Добросовестность и прозрачность действий — главный ресурс защиты менеджмента.

ПЕРВЫЕ *24 часа*



ОРГАНИЗАЦИЯ КРИЗИСНОГО УПРАВЛЕНИЯ

› Инициировать создание оперативного антикризисного штаба. Как минимум — CEO, CFO, руководитель ИТ, руководитель ИБ и юристы. При необходимости можно подключить HR и PR.

› Зафиксировать, что киберинцидент признан значимым для компании:

» приказ / служебная записка;

» короткое письмо от ИБ/ИТ с описанием факта атаки и предварительных последствий.

› Определить свою роль как CFO в штабе:

» контроль ликвидности и платежей;

» оценка влияния инцидента на выручку и исполнение обязательств;

» координация взаимодействия с банками, аудиторами, регуляторами, акционерами.

БЫСТРАЯ ОЦЕНКА МАСШТАБА ОПЕРАЦИОННЫХ И ФИНАНСОВЫХ СБОЕВ

› Получить от ИТ/ИБ короткий перечень пострадавших систем:

» ERP/«1С», казначейство, клиент-банк;

» CRM, системы склада и логистики;

» производственные системы, HR-системы.

› Оценить, какие процессы уже остановились, а какие окажутся в зоне риска в ближайшие 24–72 часа (производство, логистика, отгрузки, биллинг).

› Оценить, какие данные явно недоступны/зашифрованы/утрачены (регистры учета, базы взаиморасчетов, кадровые данные, базы заказов/клиентов).

ЛИКВИДНОСТЬ И ПЛАТЕЖИ — МИНИМАЛЬНЫЙ КОНТУР

› Проверить доступность платежных каналов:

» основной клиент-банк;

» резервные банки;

» возможность работы через отделение / бумажные документы (если критично).

› На ближайшие дни сформировать приоритизацию платежей:

» зарплаты и социально значимые выплаты;

» налоги и страховые взносы по близким срокам;

» ключевые поставщики/подрядчики, без которых встанет бизнес;

» обслуживание долга.

› Ввести временные усиленные меры контроля:

» ручная проверка платежных поручений;

» обязательная верификация изменений платежных реквизитов контрагентов по независимому каналу (звонок, сверка по ранее известным контактам);

» уведомление банка о нетипичной ситуации, чтобы снизить риск блокировок по формальным признакам.

СТАРТ ЗАЩИТЫ МЕНЕДЖМЕНТА И ФИКСАЦИЯ ДОБРОСОВЕСТНОСТИ

› Привлечь внутрикорпоративных юристов и при необходимости внешних адвокатов для оценки возможных уголовных и регуляторных рисков.

› Подготовить краткую служебную записку от CFO:

» когда стало известно об инциденте;

» какие первичные действия инициированы (по платежам, регуляторам, ликвидности, взаимодействию с ИТ/ИБ).

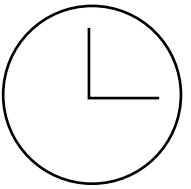
› Начать аккуратный сбор доказательной базы:

» первые письма от ИБ/ИТ;

» решения кризисного штаба;

» первые уведомления ключевым стейкхолдерам.

ПЕРВЫЕ *72 часа*



ФОРМИРОВАНИЕ КАРТИНЫ ПОСЛЕДСТВИЙ И ПЛАНА НА БЛИЖАЙШИЕ 2–3 НЕДЕЛИ

› Совместно с ИТ/ИБ подготовить более точную оценку:

» прогноз восстановления критичных систем (часы/дни/недели);

» какие данные могут быть утрачены полностью или частично.

› Определить процессы, которые нужно поддерживать любой ценой, даже вручную:

» расчет и выплата заработной платы;

» критически важные отгрузки/поставки;

» обслуживание ключевых клиентов/контрактов.

УЧЕТ, ДАННЫЕ И «ЗАМОРОЗКА БАРДАКА»

› Зафиксировать момент, после которого данные считаются потенциально повреждеными (дата/время).

› Начать инвентаризацию:

» какие участки учета пострадали (НДС, прибыль, кадры, взаиморасчеты и др.);

» какие периоды затронуты;

» какие внешние источники можно использовать для восстановления (банки, ФНС, аудитор, контрагенты).

› Определить минимальный набор функций учета, которые должны работать, даже если часть ИТ-систем недоступна:

» реестр обязательств перед контрагентами и сотрудниками;

» учет движения денежных средств (хотя бы в Excel);

» реестр налоговых и иных обязательных платежей с датами.

РЕГУЛЯТОРЫ И ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ

› Совместно с юристами решить:

» подается ли заявление о преступлении (по факту кибератаки);

» требуется ли уведомление Роскомнадзора (если затронуты персональные данные);

» нужно ли уже сейчас уведомлять/информировать ФНС и СФР, если затронут налоговый/страховой учет.

› Продумать подход к коммуникации:

» где компания обязана формально уведомить о факте инцидента;

» где имеет смысл заранее объяснить потенциальную невозможность предоставить часть документов или данных.

ВНЕШНИЕ СТЕЙКХОЛДЕРЫ

› Банки, кредиторы, страховые компании:

» при необходимости направить официальное уведомление о киберинциденте;

» объяснить возможную нестандартность операций (платежные пики, изменения контрагентов);

» если есть риск нарушения ковенантов — заранее инициировать диалог.

› Контрагенты:

» направить официальное уведомление о киберинциденте в адрес крупных бизнес-заказчиков, если это предусмотрено контрактными обязательствами.

› Внешний аудитор:

» кратко проинформировать об инциденте и возможном влиянии на учет/отчетность;

» понять, какие раскрытия и какие документы/объяснения могут потребоваться.

› Акционеры / совет директоров:

» дать честный и сдержанный апдейт: что произошло, что уже сделано, где основные риски;

» обозначить, что идет работа над оценкой ущерба и планом по снижению рисков на будущее.

ГОРИЗОНТ 2–4 НЕДЕЛИ: *восстановление учета*, ОТЧЕТНОСТИ И ДОГОВОРНЫХ ОТНОШЕНИЙ

ВОССТАНОВЛЕНИЕ УЧЕТНЫХ ДАННЫХ И ВЗАИМОРАСЧЕТОВ

› Сформировать план восстановления по основным участкам:

» бухгалтерский и налоговый учет;

» зарплатный и кадровый учет;

» взаиморасчеты с контрагентами.

› Использовать внешние источники:

» выписки и выгрузки из банков;

» данные и сервисы ФНС (декларации, сверки, личный кабинет);

» данные, ранее переданные внешнему аудитору;

» акты сверок и документы от ключевых контрагентов.

› Зафиксировать зоны, которые восстановить полностью невозможно, и сформировать по ним позицию для аудитора, ключевых контрагентов (по взаиморасчетам), ФНС и других регуляторов.

ПОДГОТОВКА К ВОЗМОЖНЫМ ПРОВЕРКАМ

› Совместно с налоговыми консультантами/юристами:

» оценить, какие участки учета наиболее уязвимы для проверок (НДС, прибыль, страховые взносы);

» продумать объяснительную позицию на случай запросов за 3 года, если документы/данные частично отсутствуют.

› Рассмотреть вопрос о создании резервов под возможные доначисления и штрафы:

» описать подход к расчету этих резервов и зафиксировать его.

РАБОТА С КОНТРАГЕНТАМИ И КЛИЕНТАМИ

› Сегментировать контрагентов и клиентов по критичности:

» кто несет наибольшие риски при срыве обязательств (штрафы, иски, потеря бизнеса, репутационный ущерб).

› Закрепить договоренности:

» допсоглашения по срокам, графикам поставок/оплат;

» договоренности о совместном восстановлении учетной информации (акты сверок, обмен копиями документов).

› По ключевым клиентам:

» оценить целесообразность компенсаций, скидок, продления условий, чтобы сохранить отношения и будущую выручку.

ВЗАИМОДЕЙСТВИЕ С АУДИТОРОМ И РАСКРЫТИЯ

› Обсудить с аудитором:

» формат и объем раскрытия информации о киберинциденте в отчетности;

» подход к оценке влияния на непрерывность деятельности (going concern);

» тесты внутреннего контроля, которые аудитор будет проводить в связи с инцидентом.

› Подготовить внутреннюю позицию:

» почему компания, несмотря на инцидент, способна продолжать деятельность;

» какие меры уже приняты, чтобы снизить вероятность повторения и уменьшить масштаб последствий.

ГОРИЗОНТ 1–3 МЕСЯЦА: ФИКСАЦИЯ УЩЕРБА, *изменение* ПРАКТИК И ДОГОВОРОВ

ОЦЕНКА УЩЕРБА И ВЛИЯНИЕ НА ПЛАНЫ

› Сформировать оценку прямых потерь:

» расходы на восстановление, подрядчиков, оборудование;

» штрафы и неустойки, выплаченные контрагентам;

» суммы выкупа данных (если компания пошла на такие платежи).

› Оценить косвенные потери:

» недополученная выручка;

» потерянные или отложенные контракты;

» снижение маржи из-за дополнительных затрат (сверхурочка, логистика, ручной труд).

› Пересмотреть бюджет и ключевые KPI:

» нужно ли формально скорректировать планы, чтобы не «наказывать» команду за провалы, вызванные последствиями кибератаки.

СТРАХОВАНИЕ И РЕГРЕСС

› Проверить, какие страховые полисы могут покрыть часть ущерба:

» киберстрахование;

» страхование ответственности директоров и должностных лиц (D&O-страхование);

» иные полисы, где киберинцидент может квалифицироваться как страховой случай.

› Оценить возможность регрессных требований к подрядчикам ИТ/ИБ:

» были ли нарушения их обязательств;

» есть ли экономический и юридический смысл в претензионной работе.

› Пересмотреть страховую политику:

» объем и лимиты киберстрахования;

» условия страхования ответственности директоров компании;

» выбор страховщика и требования к нему.

ПЕРЕСМОТР ДОГОВОРОВ С ИТ/ИБ-ПОДРЯДЧИКАМИ

› Проанализировать текущие договоры:

» есть ли реальные SLA (время восстановления, допустимый простой) и ответственность за их нарушение;

» прописаны ли требования к резервированию, регулярным тестам восстановления, планам реагирования.

› Инициировать изменения:

» ужесточить требования по SLA и ответственности;

» зафиксировать обязательные требования по резервированию и планам восстановления;

» при необходимости — сменить подрядчика.

ЧТО СОБРАТЬ В ДОСЬЕ *по инциденту*

- Описание инцидента от ИТ/ИБ:
  - даты, характер атаки, затронутые системы и данные.
- Документы по кризисному управлению:
  - приказы / служебные записки о создании штаба;
  - ключевые решения штаба, касающиеся финансов, учета, платежей, регуляторов.
- Документы CFO:
  - служебные записки о принятых мерах;
  - переписка по вопросам приоритизации платежей, ликвидности, взаимодействия с банками и регуляторами.
- Уведомления и переписка с внешними стейкхолдерами:
  - регуляторы;
  - банки и кредиторы;
  - аудиторы;
  - страховщики;
  - ключевые контрагенты и клиенты (если применимо).

Это досье — не только архив, но и база для защиты компании и менеджмента на случай, если спустя время возникнут претензии с налоговым или уголовным уклоном.

ЛИЧНАЯ *защита* ТОП-МЕНЕДЖМЕНТА

› Получить консультацию адвоката (не только внутренних юристов!) по персональным рискам ключевых лиц: CFO, CEO, ИТ-директора, директора по ИБ.

› Проверить наличие и параметры страхования ответственности директоров компании:

» покрываются ли киберинциденты и их последствия;

» нет ли критичных исключений.

› Проследить, чтобы решения по инциденту были:

» максимально коллегиальными (на уровне штаба, правления, совета директоров);

» корректно зафиксированными (протоколы, письма, резолюции).

УРОКИ НА БУДУЩЕЕ: МИНИМАЛЬНЫЙ СТАНДАРТ *готовности* ДЛЯ CFO

› Актуализировать требования к резервным копиям и срокам плановых восстановлений по критичным системам, согласованные на уровне CFO / совета директоров.

› Проверить наличие и регулярное тестирование плана продолжения бизнеса и плана реагирования на киберинцидент с участием финансового блока.

› Актуализировать договорную базу с ИТ/ИБ-подрядчиками с понятными SLA и ответственностью за простои и утрату данных.

› Актуализировать страховую политику:

» разумный уровень киберстрахования;

» адекватное страхование ответственности директоров и должностных лиц.

› Настроить получение регулярной отчетности от ИТ/ИБ для CFO и/или совета директоров:

» ключевые риски и инциденты;

» результаты тестов восстановления;

» статус реализации мер по снижению рисков.