ХардкорIT

pt

МЕТОДОЛОГИЯ

ОПРЕДЕЛЕНИЯ ПУТЕЙ И ВРЕМЕНИ АТАКИ ХАКЕРА

Издание для финансовых организаций

ЗАЧЕМ ЭТО ВСЁ?

В 31%

СЛУЧАЕВ ПРОБЛЕМА ВЫЗВАНА ОТСУТСТВИЕМ ЭФФЕКТИВНЫХ КОММУНИКАЦИЙ МЕЖДУ ПОДРАЗДЕЛЕНИЯМИ ИБ И ИТ

согласно опросам [1]

В XXI веке человечество приветствует распространение ИТ-сервисов, однако взломы и утечки обходятся бизнесу все дороже.

Количество успешных кибератак год от года растет во всех секторах экономики. Исследования[1] Positive Technologies, российской компании-лидера индустрии результативной кибербезопасности, показывают, что 93% организаций не защищены от проникновения злоумышленников во внутреннюю сеть организаций, а почти две трети организаций (63%) оказались подвержены угрозе перехвата контроля над инфраструктурой со стороны нарушителей с низкой квалификацией.

Мы в Positive Technologies знаем, как решить проблему.

Мы разработали методологию «ХардкорИТ», которая основана на математических расчетах киберустойчивости и сводит их к понятным для топ-менеджмента метрикам.

А что необходимо бизнесу, то становится важным для департамента кибербезопасности, а также понятным и осязаемым для ИТ.

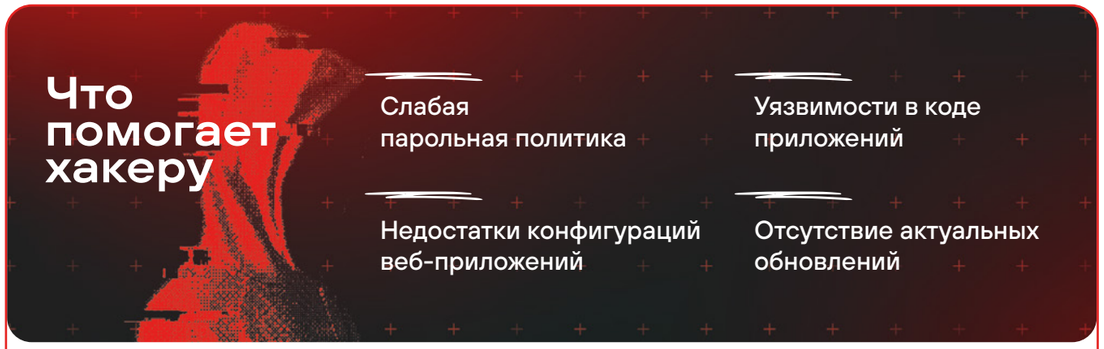
Познакомьтесь

с нашей передовой методологией, чтобы узнать, как рассчитать киберустойчивость компании

ОЦЕНКА ЗАЩИЩЕННОСТИ ИТ-ИНФРАСТРУКТУРЫ

показывает

1. Неправильно настроенная ИТ-инфраструктура является легкой добычей злоумышленников.
2. В 96% проектов организации оказались не защищены от проникновения злоумышленников в их внутреннюю сеть.
3. Самое быстрое проникновение в локальную сеть организации было осуществлено в первый день с момента начала работ.
4. В 63% организаций злоумышленник с низкой квалификацией сможет проникнуть в ЛВС извне.



Слабые места, обнаруженные в результате аудитов, **демонстрируют непонимание** того, как важно заниматься построением киберустойчивой ИТ-инфраструктуры.

ПРЕИМУЩЕСТВА ПРИМЕНЕНИЯ

ХардкорИТ

ХардкорИТ — это методология определения путей и времени атаки хакера методом анализа ИТ-инфраструктуры. Она помогает оценить киберустойчивость ИТ-инфраструктуры организации перед атаками, нацеленными на причинение недопустимого ущерба.

1

Для бизнеса

- Кибератаки не могут нанести неприемлемый ущерб бизнесу
- Снижены затраты на вывод новых продуктов и сервисов в продуктивную ИТ-инфраструктуру (Использован подход secure by design)
- Сокращаем время на переход от MVP до массового использования (сокращение time-to-market)

2

Для ИТ- и ИБ-подразделений

- Доступность сервисов не прерывается из-за кибератак
- Обоснование приоритета задач ИБ для ИТ-подразделения
- Понятное бизнесу обоснование стоимости проектов по киберустойчивости

ПЕРВЫЙ ШАГ ПРИМЕНЕНИЯ МЕТОДОЛОГИИ

определение недопустимого ущерба

Недопустимый ущерб — полученный в результате кибератаки критический урон, делающий невозможным достижение операционных и (или) стратегических целей или приводящий к значительному нарушению основной деятельности организации.

Недопустимый ущерб в финансовом секторе

примеры

Финансы

- Вывод денежных средств со счетов организации или клиентов финансовой организации
- Остановка операционных процессов финансовой организации н критичный срок (определяется самой организацией или внешним регулятором)
- Недоступность цифровых финансовых сервисов для клиентов
- Исользование инфраструктуры и цифровых сервисов финансовой орагнизации для выполнения атак на клиентов и партнеров

примеры

Технологические компании

- Перебои в работе или недоступность платформ и клиентских сервисов, корпоративной инфраструктуры
- Утрата исходного кода или внедрение уязвимостей и программных закладок в исходный код разрабатываемых продуктов
- Недоступность электронных сервисов для клиентов и партнеров на срок более 1 дня
- Подмена транслируемого контента, в том числе фальсификация результатов участников мероприятия

СЛЕДУЮЩИЙ ЭТАП

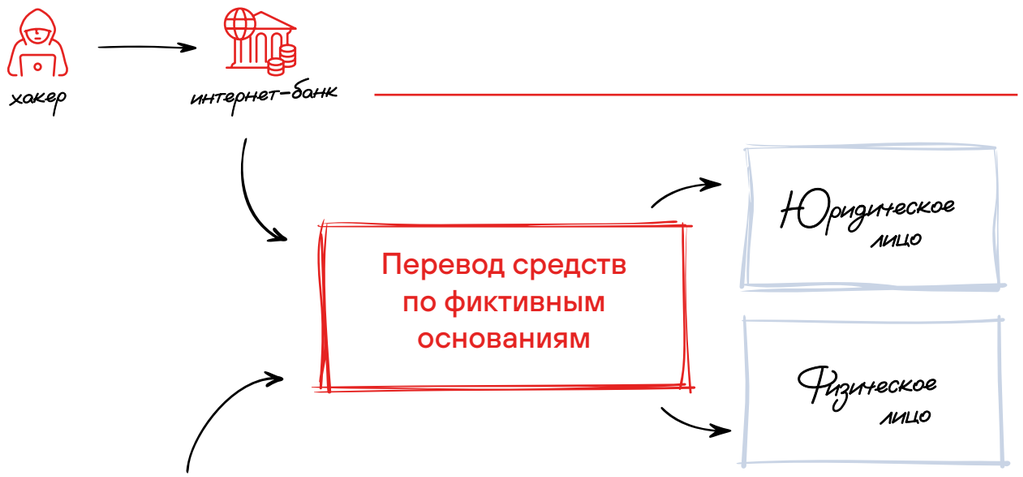
→ *определение сценариев*

Определяются сценарии, следуя которым злоумышленник может реализовать ситуацию недопустимого ущерба.

Сценарии недопустимого ущерба для банковской инфраструктуры

Сценарий 1

Массовый вывод денег со счетов физических лиц



Сценарий 2

Вывод денег со счета юридического лица

Как сделать финтех киберустойчивым к недопустимому ущербу с помощью методологии ХардкорLIT

TTA > TTC

ВРЕМЯ АТАКИ ДОЛЖНО ПРЕВЫШАТЬ ВРЕМЯ ЛОКАЛИЗАЦИИ

Метрики киберустойчивости организаций финансового сектора

Жизненный цикл инцидента в соответствии с определением реагирования на ИИБ из NIST 800-61 Rev 2*:

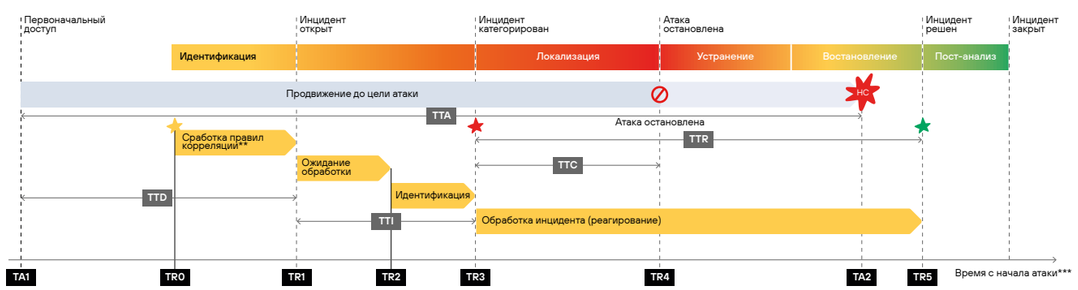
- Подготовка
- Идентификация инцидента
- Локализация угрозы
- Устранение угрозы
- Восстановление (снижение последствий реализации угрозы)
- Действия после инцидента

Формула TTA > TTC заключает в себе наиболее важные метрики, которые напрямую влияют на исход инцидента. Время, которое затратит злоумышленник на совершение атаки Time-To-Attack, должно быть больше, чем время, которое служба ИБ потратит на обнаружение, локализацию и прекращение этой атаки Time-To-Contain.

Добиться этого можно двумя путями: как удлиняя и усложняя путь хакера, а также делая его продвижение более заметным, так и сокращая время обнаружения атаки и реагирования вплоть до остановки хакера и восстановления деятельности компании.

Развернув жизненный цикл инцидента на прямой график, мы нанесли на него стадии атаки и реагирования для наибольшей наглядности.

Метрика	Определение
TTD	Время обнаружения – время от момента первоначального доступа агента угрозы в сеть организации до окончания обнаружения атаки.
TTI	Время идентификации – время от момента первоначального доступа агента угрозы в сеть организации до определения шагов по реагированию.
TTA	Время атаки – время от первоначального доступа до момента нанесения недопустимого ущерба.
TTC	Время локализации – время от категоризации инцидента (т.е. когда становится ясно, что делать) до окончания локализации (блокирования и изоляции агента угрозы).
TTR	Время реагирования – время от начала локализации до перевода инцидента в статус «Решён».



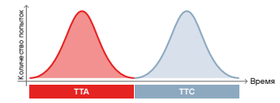
* NIST Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide. nist.gov

** В SIEM или иного другого правила в СЗИ, предназначенного для обнаружения атаки.

*** Длина отрезков на временной шкале не соответствует реальной длительности этапов реагирования на ИИБ и приведена только для иллюстрации общей последовательности этапов и их относительного расположения.

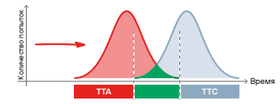
**** Относительно вех на графике

Исходный случай
Всегда опаздываем



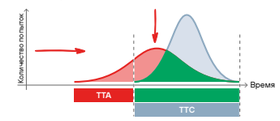
Атакующий всегда достигает своей цели, реагирование происходит слишком поздно

Вариант 1
Укрепили периметр, немножко успеваем



Замедлили атаку на периметре
(атакующему надо долго вести разведку и предпринимать неоднократные проникновения).

Вариант 2
Укрепили периметр, замедлили и сделали более заметной атаку. Успеваем гораздно больше



Удлинили и замедлили атаку. Распределение попыток атаки не только сдвинулось вправо, но и «сплющилось»

Моделируем сценарии атак и реагирования

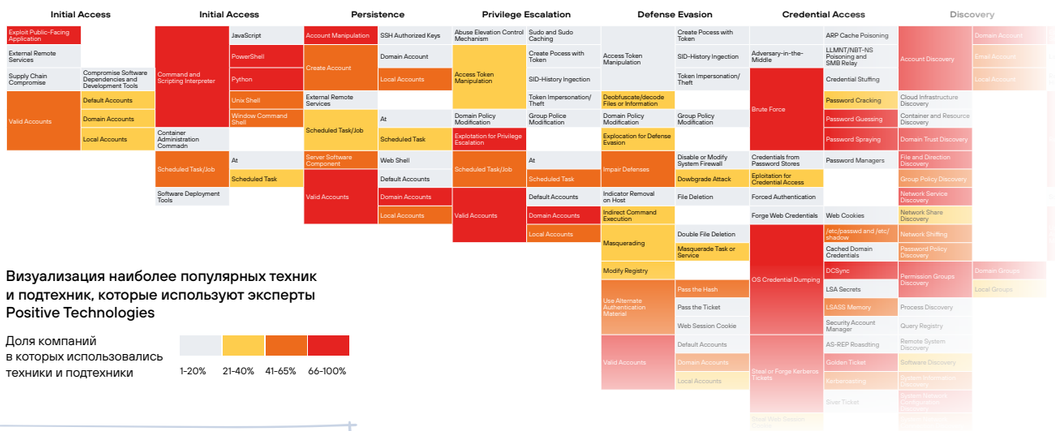
Определив недопустимый ущерб, мы должны изменить ИТ-инфраструктуру таким образом, чтобы путь атакующего в ней был максимально сложным и «шумным», а затем поддерживать это состояние. Для такой трансформации мы используем преимущественно средства из арсенала ИТ – харденинг.

С помощью этого мощного инструмента можно привести компанию из состояния, где ИТ-инфраструктура проницаема для злоумышленников, а служба безопасности не замечает кибератаку, в состояние, когда усилен периметр, выполнены правильные настройки сетевого оборудования, пишутся логи и хватает места для их хранения. При этом путь атакующего становится сложным и заметным, а у службы ИБ есть время для обнаружения хакера и начала ответных мер.

На этом этапе мы проектируем сценарии атак и реагирования as is и в целевом состоянии.

Рассчитываем защиту ИТ-инфраструктуры с помощью тепловой карты MITRE[2]

MITRE ATT&CK — широко распространенный справочник техник, тактик, процедур, реестра действий по детектированию и предотвращению атак, который регулярно обновляется международным сообществом экспертов.



Визуализация наиболее популярных техник и подтехник, которые используют эксперты Positive Technologies

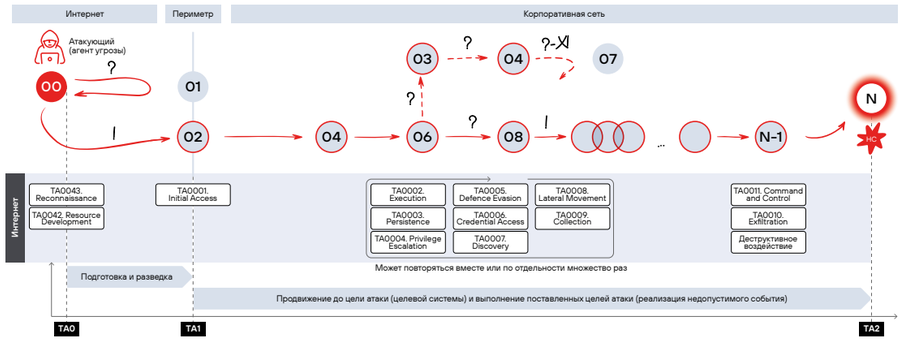
Доля компаний в которых использовались техники и подтехники: 1-20% 21-40% 41-65% 66-100%

TTP	Min	Max
TTP1	10 мин	2 часа
TTP2	15 мин	24 часа
TTP3	30 мин	30 часов
TTP8	10 мин	12 часов

Проработав визуализацию покрытия тактик и приемов MITRE ATT&CK, определяем профили мониторинга и харденинга, а также приоритизируем применение контролей для противодействия злоумышленникам.

Продвижение атакующего

Смотрим на путь хакера через призму тепловой карты



Данная схема сознательно упрощена для иллюстрации следующих далее понятий.

- 00 Рабочая станция атакующего
- Граница корпоративной сети
- 01 Узел, не затронутый атакой
- Успешное продвижение атакующего
- ? Сбор данных, разведка
- 02 Узел, затронутый атакой
- Неуспешное продвижение атакующего
- ! Успешные действия
- N-1 Ключевая система
- N Целевая система
- ?-✕ Дальнейшее продвижение невозможно/нецелесообразно

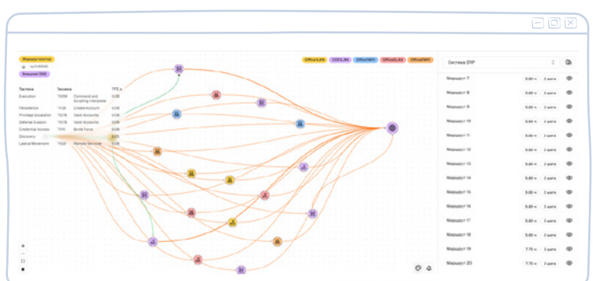
На схеме продвижения атакующего показаны возможные варианты развития атаки. Точкой отсчета является момент проникновения хакера через периметр организации или условный периметр опубликованного сервиса.

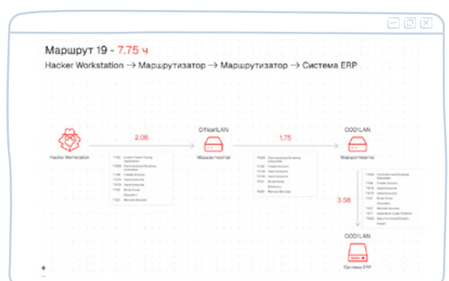
Далее у злоумышленика есть конечное множество маршрутов к целевой системе. определение маршрута атакующего происходит на основе доступных тактик и техник (далее TTP) на конкретном узле. Происходит расчет времени применения TTP. Как итог — формируются все возможные маршруты, вероятное время их прохождения, используемые TTP и инструментарий.

Моделируем атаки на ИТ-инфраструктуру

Собрав цифровой отпечаток ИТ-инфраструктуры компании, проводим моделирование атак и отвечаем на следующие вопросы:

- **Как определить маршрут атаки?**
- **Как посчитать время атаки?**
- **Как определить системы, через которые злоумышленники будет приоритетно атаковать?**
- **Как определить техники, которые будут использоваться злоумышленником?**
- **Как настройки безопасности влияют на время атаки?**
- **Как настройки безопасности влияют на маршрут атаки?**
- **Как настройки безопасности влияют на используемые техники?**

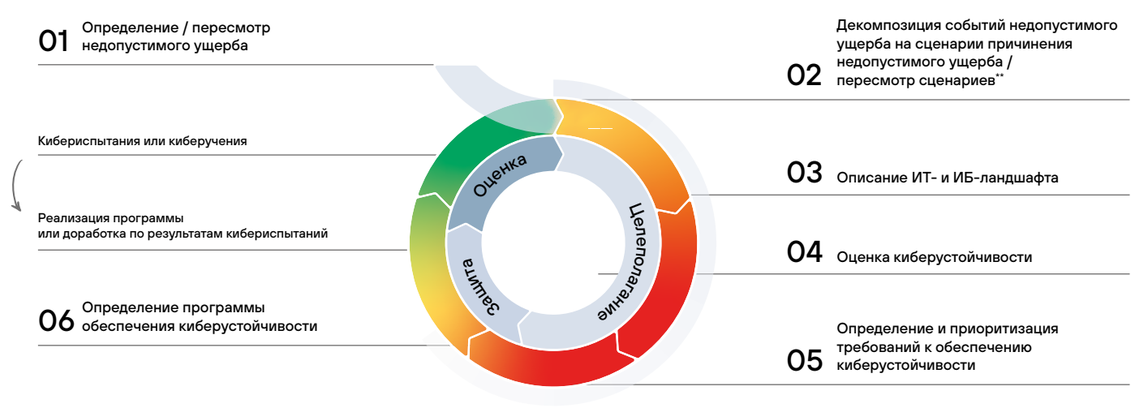




Создаем жизненный цикл обеспечения киберустойчивости в методологии ХардкорИТ

Обновление ИТ-инфраструктуры с применением превентивных и обнаруживающих* контролей (релевантных сценариям реализации недопустимого ущерба) помогает удлинить время атаки и сделать ее заметнее. В результате реагирование исключает реализацию недопустимого ущерба.

Регулярная оценка эффективности предлагаемых мер и реализация программы трансформации помогает компании достичь состояния киберустойчивости.



Шаг	Что дает бизнесу
01	Знание о том, где и зачем нужна информационная безопасность, чтобы тратить ресурсы на защиту только необходимых бизнес-систем.
02	Знание сценариев, ключевых и целевых систем делают процесс защиты более осознанным, точечным и менее затратным.
03	Определение самых проблемных ИТ-активов ключевых и целевых систем, функциональных областей их работы, на которых нужно сфокусировать ресурсы по защите
04	Расчет интуитивно понятных бизнесу метрик кибербезопасности, определение наиболее приоритетных маршрутов злоумышленников для защиты целевых систем. Определение готовности противостоять реализации недопустимых событий.
05	Определение набора инициатив на основе моделирования атак на бизнес-системы. Приоритизация шагов по обеспечению киберустойчивости на основе аналитики моделирования атак.
06	Формирование программы трансформации, сбалансированной с точки зрения затрат бизнеса для обеспечение состояния киберустойчивости. Программа трансформации создается с учетом инициатив бизнес-стратегии и ИТ-стратегии.

* По классификации FAIR. В этом документе будет использоваться классификация FAIR,

** Этот этап может пропускаться – в случае, если заказчик по каким-то причинам не может сформулировать НС, но в состоянии сразу определить ЦС и КС.

РЕЗУЛЬТАТЫ ПРОЕКТА

Шаги проекта	Deliverable	Разделы
01. Определение/ пересмотр недопустимого ущерба **02.** Декомпозиция недопустимого ущерба на сценарии реализации недопустимого ущерба	**D00.** Краткое описание методологии (PPT/DOC) **D01.** Реестр недопустимого ущерба (DOC)	**D00.** **Краткое описание методологии – краткое описание (без утверждения), включая термины и определения** **D01.** **Реестр недопустимого ущерба (документ на 3-4 страницы):** • Введение • Список недопустимого ущерба с параметрами (время, суммы, количество, география) • Список сценариев реализации недопустимого ущерба с ключевыми и целевыми системами и описанием сценария • Общий список целевых и ключевых систем
03. Описание ИТ- и ИБ-ландшафта	**D02.** Описание ИТ- и ИБ-ландшафта (PPT/DOC)	**Документ на 15-20 страниц описывает:** • ИТ-ландшафт – ИТ-инфраструктуру (маппинг ключевых и целевых систем на функциональные области деятельности компаний и наличие ИТ-инфраструктурных и ИБ-систем в ИТ-ландшафте по согласованному фреймворку) – Общую топологию локальной вычислительной сети (сегменты и их связность) и сетевое оборудование – Типовые конфигурации серверов – Системы хранения данных – Систему резервного копирования – Систему виртуализации – Систему мониторинга ИТ – Типовые конфигурации рабочих станций и иных оконечных устройств – Службу каталога – Электронную почту и другие каналы электронной коммуникации (системы видеоконференцсвязи, корпоративные мессенджеры и пр.) – Архитектуру целевых систем • ИБ-ландшафт – Оценку зрелости ИБ по 10 доменам методики Positive Technologies – Системы мониторинга ИБ (обнаруживающие меры) – Меры по реагированию на инциденты ИБ – Превентивные меры – Применение мер к целевым системам и элементам ИТ-ландшафта – Параметры безопасности целевых систем • Список обнаруженных проблем и расхождений с известными исполнителю лучшими практиками

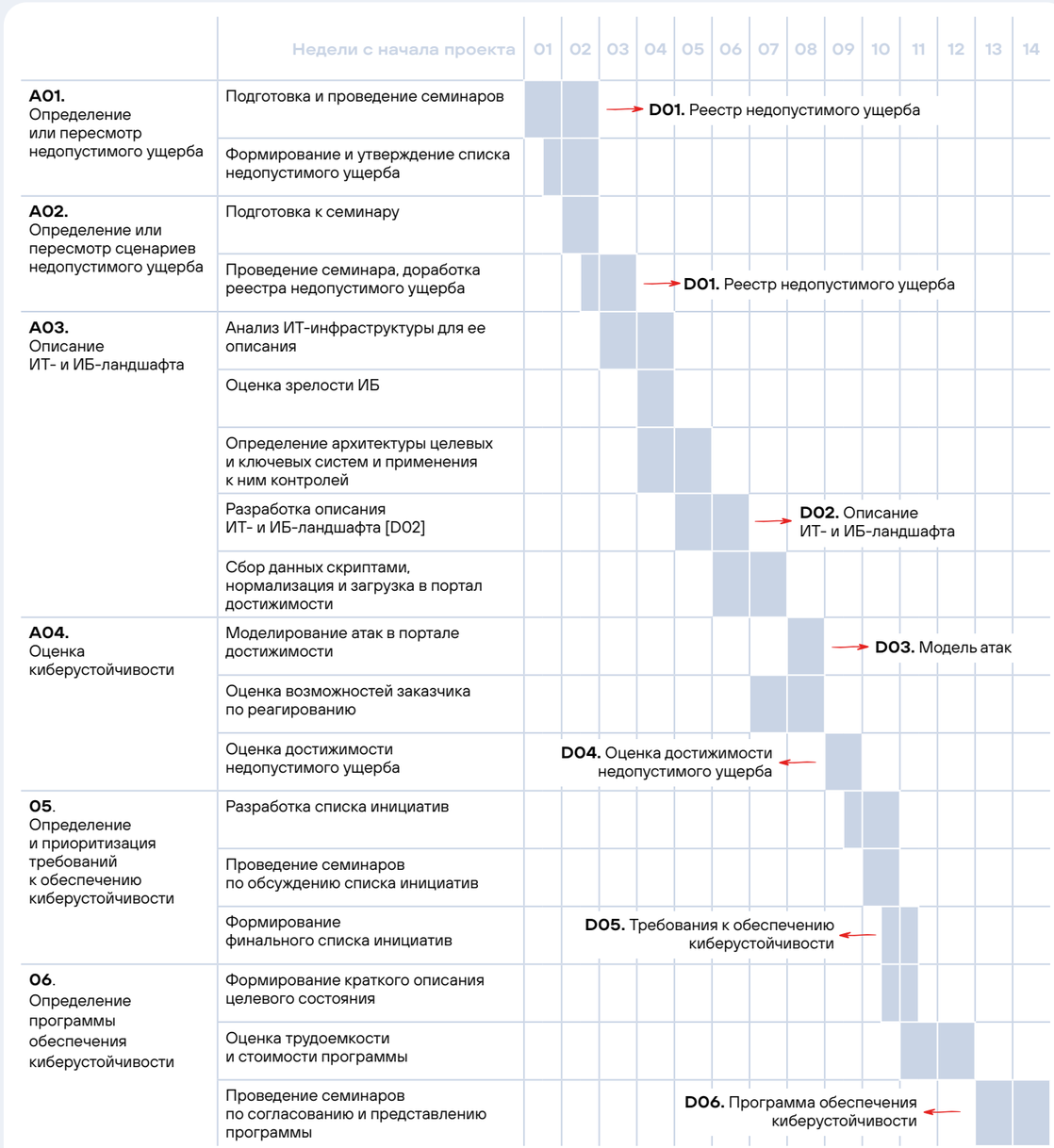
Набор документации →

в рамках проработки этих этапов позволяет полностью закрыть потребности в формировании стратегии трансформации ИТ-инфраструктуры.

Шаги проекта	Deliverable	Разделы
04. Оценка киберустойчивости	**D03.** Модель атак (PPT/DOC) **D04.** Метрики достижимости (PPT)	**D03.** **Модель атак на 15-20 страницах описывает:** • Реестр недопустимых событий и сценариев их реализации • Категории злоумышленников (агентов угрозы) и их возможности • Предположения и допущения • Точки входа в сеть – Ресурсы в сети Интернет – Сети Wifi – Рабочие станции в локальной сети – Периферийные устройства рабочих станций и серверов локальной сети • Маршруты атаки целевых систем (не более 3 цепочек на 1 событие, вызывающее недопустимый ущерб) – Используемые техники – Выполняемые тактики – Граф атаки – Оценка времени атаки **D04.** **Оценка достижимости недопустимого ущерба** • Маршруты атаки • Сравнение времени атаки с текущим временем локализации инцидента в организации заказчика
05. Определение и приоритизация требований к трансформации ИТ	**D05.** Требования к трансформации (Excel/PPT)	• Список инициатив (предложений по внедрению рекомендаций), сгруппированный в проекты • Маппинг инициатив на проблемы [D02], оценка сложности, стоимости и трудоемкости реализации инициатив • Приоритизация (фильтрация) инициатив на основе метрик: – Влияние на TTA – Влияние на TTC/TTR – Влияние (улучшение) на контроли – Quick wins
06. Определение программы трансформации	**D06.** Программа трансформации (PPT)	**Документ на 15-20 страниц описывает:** • Список проблем • Сравнение TTA и TTC/TTR для сценариев реализации НС • Инициативы/проекты • Маппинг инициатив/проектов на проблемы • Оценку влияния инициатив на метрики (bubble charts) • Дорожную карту трансформации на 3 года (график проектов) • Оценки трудоемкости/стоимости инициатив и cash flow на 3 года

ПРИМЕРНЫЙ ПЛАН ПРОЕКТА

В среднем проект по повышению киберустойчивости на основе методологии ХардкорИТ занимает 3,5 месяца и завершается семинарами, на которых заказчик получает все отчетные документы и знакомится с дальнейшими рекомендациями.



СТРАТЕГИЯ ОБЕСПЕЧЕНИЯ КИБЕРУСТОЙЧИВОСТИ

Итогом работа по проекту ХардкорИТ становится программа трансформации компании. Эта программа включает в себя ряд инициатив, анализ их влияния на расчетные метрики киберустойчивости, расчет сложности, сроков и бюджетной оценки.

В первую очередь инициативы направлены на модернизацию ИТ-инфраструктуры, на использование собственных, встроенных механизмов защиты, а затем на использование дополнительных систем и сервисов защиты.

Таким образом, реализация всех инициатив приводит к невозможности реализации недопустимого ущерба.

Инициативы / Проекты	Влияние на TTA	Влияние на TTC	Стоимость	Сроки	Сложность	Приоритет
И1. Харденинг ИТ-инфраструктуры	высокое	низкое	xxx	xx	4	1
И2. Модернизация сети	высокое	среднее	xxx	xx	1	1
И3. Модернизация программной ИТ-инфраструктуры	среднее	низкое	xxx	xx	2	2
И4. Обучение сотрудников киберграмотности	низкое	низкое	xxx	xx	2	1
И5. Построение защищенного домена	высокое	низкое	xxx	xx	3	2
И6. Автоматизация патч-менеджмента	низкое	низкое	xxx	xx	3	2
И7. Внедрение системы управления уязвимостями	низкое	низкое	xxx	xx	3	1
И8. Централизация управления активами	среднее	низкое	xxx	xx	3	1
И9. Реализация лучших практик SDLC	высокое	низкое	xxx	xx	1	2
И10. Внедрение решений класса NTA, WAF	низкое	низкое	xxx	xx	3	1
И11. Внедрение EDR	среднее	среднее	xxx	xx	2	1
И12. Построение SOC	среднее	высокое	xxx	xx	4	2
И13. Модернизация двухфакторной аутентификации	высокое	низкое	xxx	xx	4	2
И14. Внедрение защиты от фишинга	высокое	низкое	xxx	xx	2	2
И15. Проведение киберучений	среднее	высокое	xxx	xx	3	3

РЕАЛИЗУЕМ ПРОГРАММУ КИБЕРУСТОЙЧИВОСТИ

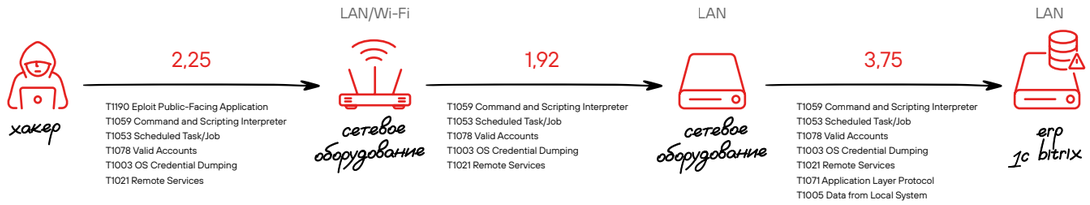
ХардкорИТ на практике

От этого состояния ...

Недопустимый ущерб

Несанкционированный доступ к бизнес-системе ERP

Время атаки 7,92 часа

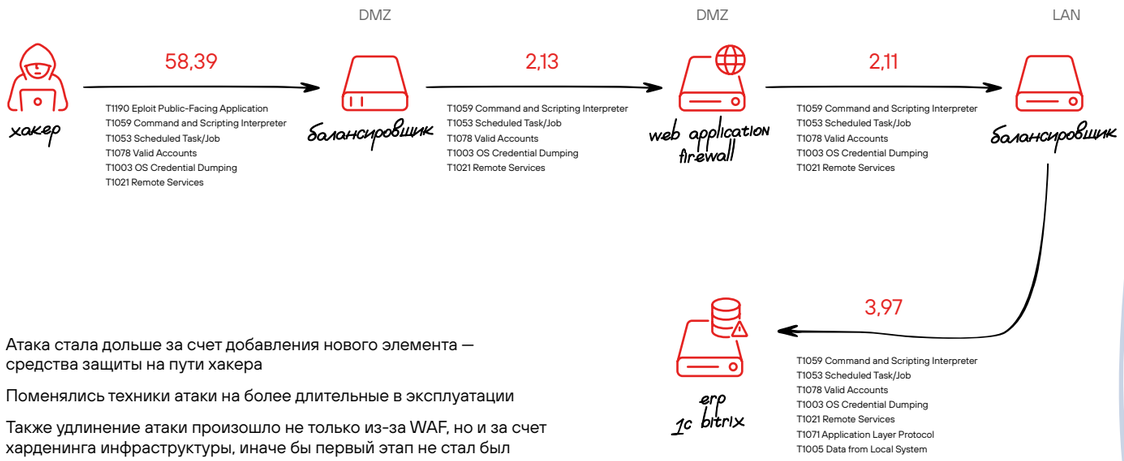


... к этому состоянию

Недопустимый ущерб

Несанкционированный доступ к бизнес-системе ERP

Время атаки 66,6



Атака стала дольше за счет добавления нового элемента — средства защиты на пути хакера

Поменялись техники атаки на более длительные в эксплуатации

Также удлинение атаки произошло не только из-за WAF, но и за счет харденинга инфраструктуры, иначе бы первый этап не стал был дольше на порядок.

ПОЧЕМУ POSITIVE TECHNOLOGIES?

20+

ЛЕТ ОПЫТА ИССЛЕДОВАНИЙ И РАЗРАБОТОК

2200+

ИНЖЕНЕРОВ ПО ИБ, РАЗРАБОТЧИКОВ, АНАЛИТИКОВ И ДРУГИХ СПЕЦИАЛИСТОВ

2500+

ЭКСПЕРТОВ В НАШЕМ ИССЛЕДОВАТЕЛЬСКОМ ЦЕНТРЕ БЕЗОПАСНОСТИ

250+

ОБНАРУЖЕННЫХ УЯЗВИМОСТЕЙ НУЛЕВОГО ДНЯ В ГОД

200+

АУДИТОВ БЕЗОПАСНОСТИ КОРПОРАТИВНЫХ СИСТЕМ ДЕЛАЕМ ЕЖЕГОДНО

50%

ВСЕХ УЯЗВИМОСТЕЙ В ПРОМЫШЛЕННОСТИ И ТЕЛЕКОМАХ ОБНАРУЖИЛИ НАШИ ЭКСПЕРТЫ

НАШ ИНФРАСТРУКТУРНЫЙ ЦЕНТР ОБЛАДАЕТ ШИРОКОЙ ЭКСПЕРТИЗОЙ В ИТ

ИТ-СИСТЕМЫ И СЕРВИСЫ POSITIVE TECHNOLOGIES НЕПРЕРЫВНО ВЫСТАВЛЕНЫ НА БАГБАУНТИ, В ТОМ ЧИСЛЕ НА АРТ-БАГБАУНТИ *(ВОЗНАГРАЖДЕНИЕ 60 МЛН РУБЛЕЙ, 0 СДАННЫХ ОТЧЕТОВ)*

создаем продукты и решения

проводим аудиты безопасности

расследуем инциденты

исследуем угрозы

разрабатываем стандарты и методологии

Для заметок

сканируй QR и скачивай другие наши брошюры!

Брошюра ХардкорИТ

РезБез

Хардеринг Microsoft Exchanfe

ПОЛЕЗНЫЕ ССЫЛКИ

ptsecurity.com

Positive Technologies — лидер в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики.

Наши технологии используют более 4000 организаций по всему миру.

Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 205 тысяч акционеров.