



ПОДХОД

путь к киберустойчивости

МИРОВАЯ И РОССИЙСКАЯ РЕАЛЬНОСТЬ КИБЕРУГРОЗ



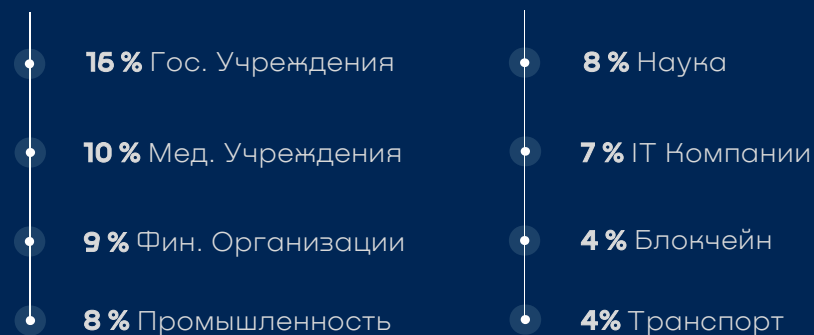
4,45 млн. долл

Составила средняя мировая стоимость утечки данных в 2023, что на 15% больше, чем за 3 года.**

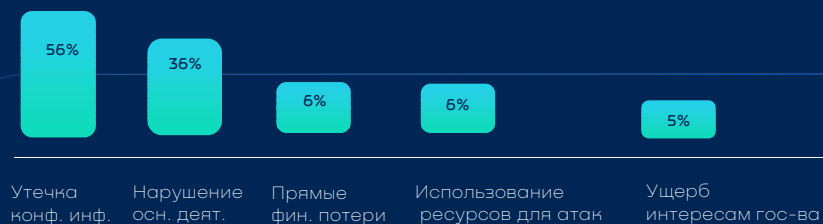
♦ Популярные методы успешных атак:



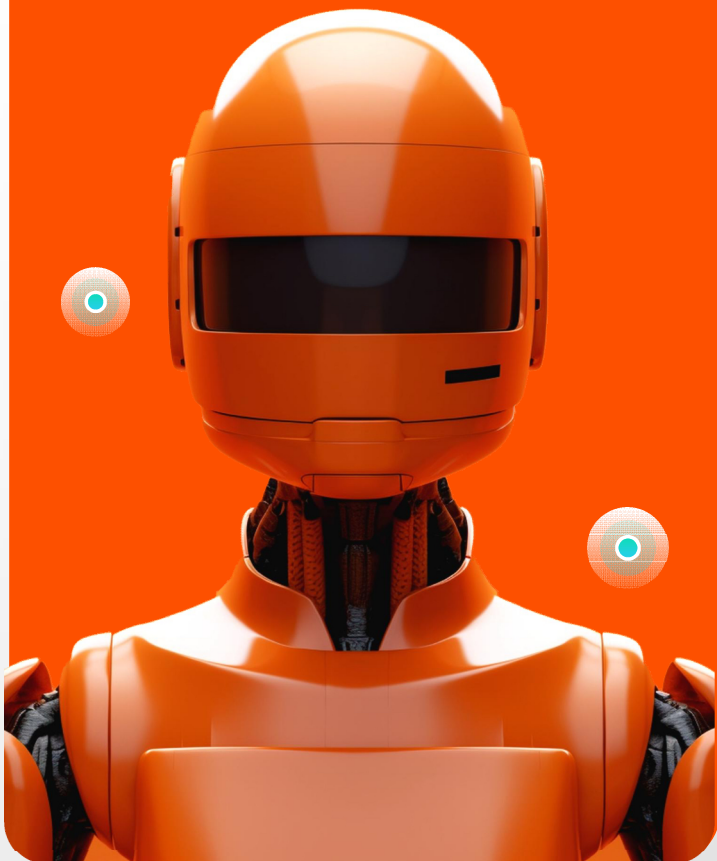
*по данным Positive Technologies
**по данным специалистов IBM



♦ Последствия атак для организаций:



СТРУКТУРА ПОДХОДА ПУТЬ К КИБЕРУСТОЙЧИВОСТИ



01 Оценка уровня киберустойчивости:

Цифровая архитектура
Особенности и риски бизнеса

- ✓ Модели оценки негативного влияния
- ✓ Проведение первичных испытаний

01

02 Дизайн целевой архитектуры:

Прототипы целевой конфигурации
ИТ-архитектуры и сегментов



Design in process...

Архитектура ИТ-инфраструктуры

Состав логических и физических сегментов

02

03 Трансформация и обеспечение процессов

Модели оценки влияния на устойчивость ИТ
активов, процессы и практики достижения
целевого состояния

- Активы и конфигурационные единицы
- Средства автоматизации

03

04 Подготовка и обучение персонала

Тренировочные центры,
платформы и менторство

ИТ

ИБ



сотрудники

04

05 Независимая оценка устойчивости

Методики проведения испытаний,
эксперты и исследователи

- ✓ Поддержка целевого уровня киберустойчивости
- ✓ Поддержка готовности эксплуатирующего персонала

05



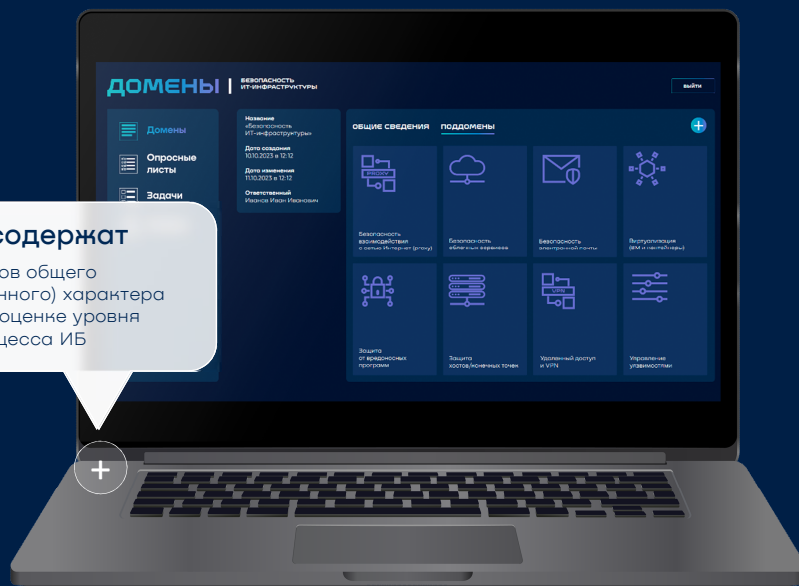
ЭТАП 1. МОДЕЛЬ ОЦЕНКИ НЕГАТИВНОГО ВЛИЯНИЯ



Содержит методику оценки 15 доменов (областей ИБ)

Домены содержат

блоки вопросов общего (организационного) характера и вопросы по оценке уровня зрелости процесса ИБ



Наличие СЗИ

Степень покрытия

Выполнение требований ИБ

Контроль и метрики ИБ



ЭТАП 1. МОДЕЛЬ ОЦЕНКИ НЕГАТИВНОГО ВЛИЯНИЯ



✦ Экспертный опыт проведения аудитов ИБ команды Innostage

большой опыт

навык применения лучших практик

опыт применения международных и российских практик для оценки состояния ИБ,

зарекомендовавших себя при проведении аудитов: ISO/IEC 27001/27002:2013, CMMI, ISF (ведущая компания в области экспертизы ИБ),

российские регуляторные и отраслевые методики.





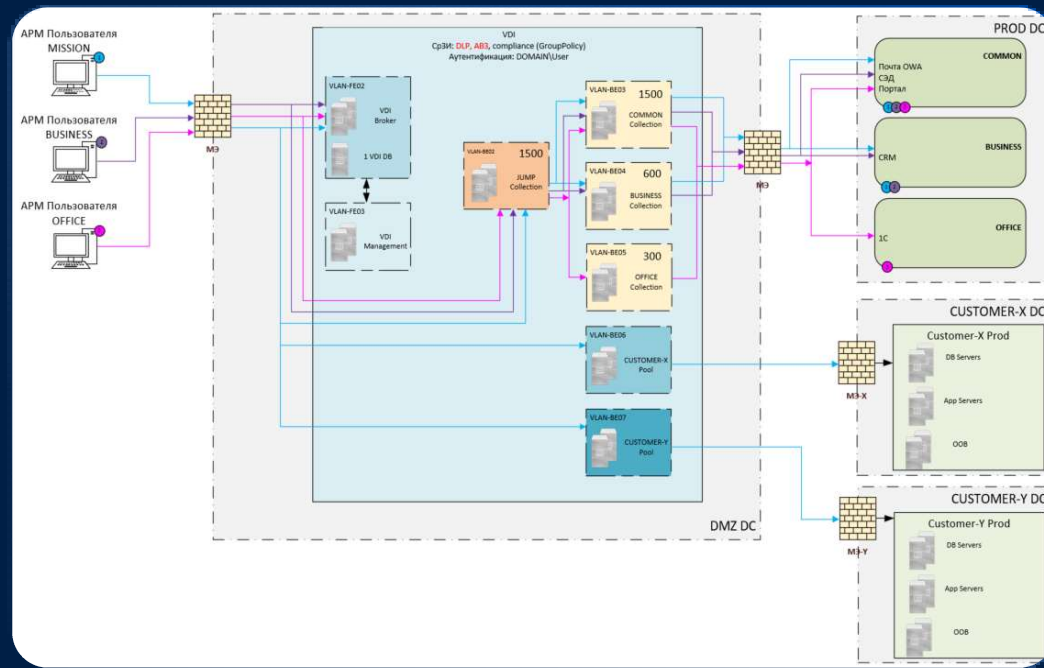
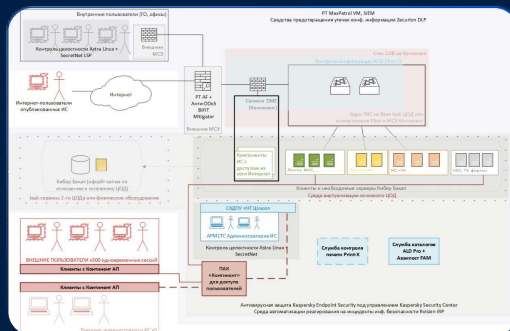
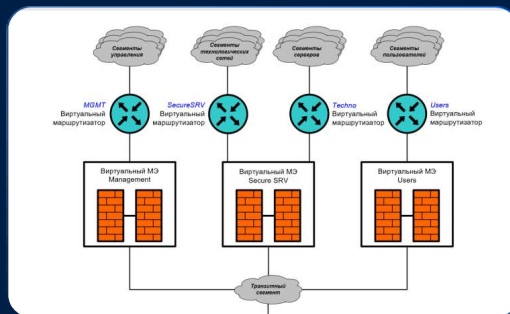
ЭТАП 2. ДИЗАЙН ЦЕЛЕВОЙ АРХИТЕКТУРЫ. ВЗАИМОСВЯЗЬ АРТЕФАКТОВ



Шаблоны архитектур

Проектный опыт

Проверенный подход по построению целевой архитектуры





ЭТАП 3. ТРАНСФОРМАЦИЯ И ОБЕСПЕЧЕНИЕ ПРОЦЕССОВ




✦ Структура модели данных «Киберустойчивость»





ЗНАЧИМОСТЬ ОБЪЕКТА ЗАЩИТЫ



 <p>Типовой элемент ИТ-инфраструктуры</p>		Базовые меры, необходимые для создания видимости и устойчивости основных элементов ИТ инфраструктуры
 <p>Входят в состав ключевого ИТ-сервиса</p>		Оптимальный набор мер, направленных на повышение видимости и устойчивости элементов ИТ инфраструктуры и ключевых ИТ сервисов
 <p>Входят в состав критичной автоматизированной системы</p>		Меры, направленные на повышение видимости и надежности ключевых автоматизированных систем
 <p>Является участником ключевого бизнес-процесса</p>		Меры, направленные на создание видимости и непрерывности ключевых бизнес-процессов, клиентских сервисов и услуг
 <p>Требуется максимальная устойчивость актива</p>		Продвинутое меры для максимально достижимой устойчивости и защищенности



ЭТАП 3. ТРАНСФОРМАЦИЯ И ОБЕСПЕЧЕНИЕ ПРОЦЕССОВ



Ключевые аспекты процессов





ИНВЕНТАРИЗАЦИЯ



КРИТЕРИЙ 1



КРИТЕРИЙ 5



Назад

Инвентаризация и классификация
конфигурационных единиц

Инвентаризация правил
межсетевого экранирования

Инвентаризация
учетных данных

Инвентаризация
IP-сетей

Пример реализации





Этап 3. Трансформация и обеспечение процессов: примеры реализуемости процессов и задач



ИТ-актив	Направление	Процессы и задачи	Классы решений	Технические решения
АСО/Маршрутизаторы/М СЭ	Инвентаризация	Инвентаризация и классификация конфигурационных единиц	Сканер уязвимостей	XSpider, Nessus
			Сканер периметра	ASM, непрерывный сканер периметра
			CMDB	Netbox
		Инвентаризация правил межсетевого экранирования	SIEM	MaxPatrol SIEM
			CMDB	Netbox
			Менеджер конфигураций	Нетхаб
			Ручной аудит	
		Инвентаризация учетных данных	Ручной аудит	
			SIEM	MaxPatrol SIEM
		Инвентаризация IP-сетей	CMDB	Netbox
Менеджер конфигураций	Нетхаб			



КОНТРОЛЬ ИЗМЕНЕНИЙ, СООТВЕТСТВИЯ ПОЛИТИКАМ



КРИТЕРИЙ 1



Контроль обновлений

Контроль сетевых доступов и сервисов

Контроль соответствия политикам ИБ/НПА

КРИТЕРИЙ 5



Контроль доступа администраторов

Контроль изменений конфигураций

Контроль обновлений

Контроль сетевых доступов и сервисов

Контроль соответствия
политикам ИБ/НПА

Контроль метрик производительности



ПРОВЕРКА ЗАЩИЩЕННОСТИ / ОТКАЗОУСТОЙЧИВОСТИ



КРИТЕРИЙ 1



Проверки на наличие избыточных сервисов

Проверки нарушения сегментации сетей

КРИТЕРИЙ 5



Проверки несоответствия конфигураций эталонным

Проверка криптостойкости

Проверки избыточных прав и стойкости аутентификации

Проверка соответствия подключаемых к сети устройств

Проверки на наличие избыточных сервисов

Проверка уязвимостей

Проверки на "присутствие" легитимных сервисов

Проверки нарушения сегментации сетей

Проверка переключения на резервные конфигурационные единицы (кластеризация, ЗИП)



ОБЕСПЕЧЕНИЕ ЗАЩИТЫ / НЕПРЕРЫВНОСТИ



КРИТЕРИЙ 1



Сегментация сетей

Защита доступа в сеть-интернет

КРИТЕРИЙ 5



Защита от DDOS

Защита от нелегитимного
изменения конфигураций

Управление уязвимостями

Резервирование
конфигурационных единиц

Резервирование
конфигураций

Сегментация сетей

Защита от сетевых
вторжений и атак

Защита от VLAN Hopping

Защита от
несанкционированного
доступа

Защита доступа
в сеть-интернет



МОНИТОРИНГ



КРИТЕРИЙ 1



КРИТЕРИЙ 5



Управление журналами аудита (логи)

Мониторинг сетевых взаимодействий

Мониторинг событий ИБ

Мониторинг работоспособности
(доступность, производительность
и Health Check)

Мониторинг изменений



РЕАГИРОВАНИЕ / ВОССТАНОВЛЕНИЕ



КРИТЕРИЙ 1



КРИТЕРИЙ 5



Реагирование на компьютерные
атаки и отклонения

Восстановление эталонной
конфигурации

Восстановление отказоустойчивой
конфигурации



ИТ-АКТИВЫ: ПРИМЕРЫ РЕАЛИЗУЕМОСТИ ПРОЦЕССОВ И ЗАДАЧ



каналы передачи данных, серверы



бизнес системы (продуктивные системы), ВЕБ/API сервисы



инфраструктурные сервисы, системы взаимодействия пользователей



сервисы удаленного доступа



привилегированные и рядовые пользователи



СУБД\БД\DATA lake



КАНАЛЫ ПЕРЕДАЧИ ДАННЫХ. СЕРВЕРЫ



КАНАЛЫ

Инвентаризация

- Инвентаризация каналов связи
- Инвентаризация используемых протоколов и их классификация
- Инвентаризация параметров шифрования

Контроль изменений, контроль соответствия политики

- Контроль появления новых каналов связи
- Контроль восстанавливаемости канала связи
- Контроль изменений параметров шифрования

Проверка защищенности/отказоустойчивости

- Проверка криптостойкости
- Проверка резервирования каналов связи

Обеспечение защиты/непрерывности

- Защита от DDoS
- Криптографическая защита каналов связи
- Резервирование каналов связи
- Защита от НСД

Мониторинг

- Мониторинг работоспособности (доступность, производительность, Health Check)

Реагирование/Восстановление

- Противодействие DoS/DDoS
- Переключение на резервный канал связи
- Восстановление/переключение на каналы криптографической защиты

Расследование

СЕРВЕРЫ

Инвентаризация

- Инвентаризация съемных устройств
- Инвентаризация установленного ПО
- Инвентаризация и классификация АРМ/Серверов

Контроль изменений, контроль соответствия политики

- Контроль подключения съемных устройств
- Контроль изменения критичных конфигураций ОС
- Контроль обновлений ОС и ПО
- Контроль доступа к критичным параметрам конфигурации ОС
- Контроль эталонных образов для развертывания (АРМ, Серверы)
- Контроль целостности критичных служб

Проверка защищенности/отказоустойчивости

- Проверка резервных копий на работоспособность
- Проверка наличия избыточных сервисов
- Проверка уязвимостей
- Проверка наличия избыточных АРМ/Серверов
- Управление ресурсами критичных систем

Обеспечение защиты/непрерывности

- Защита от вредоносных программ
- Резервирование конфигураций критичных АРМ/Серверов
- Шифрование жестких дисков
- Ужесточение конфигураций безопасности
- Защита от несанкционированного доступа
- Управление приманками/ловушками
- Управление уязвимостями

Мониторинг

- Мониторинг событий ИБ
- Мониторинг изменений критичных конфигураций ОС
- Мониторинг работоспособности Серверов/АРМ
- Управление журналами аудита (логи)

Реагирование/Восстановление

- Восстановление из резервных копий (АРМ, Сервера)
- Управление компьютерными инцидентами и отклонениями

Расследование



ЭТАП 4. ПОДГОТОВКА И ОБУЧЕНИЕ ПЕРСОНАЛА



Тренировочные центры, платформы и менторство



Все сотрудники компании
Программа повышения осведомлённости



Эксплуатирующий персонал
Киберучения

В результате Level Up

Отточенные навыки и практические знания, опыт взаимодействия

Платформа для обучения сотрудников

- Задания, курсы, отчеты
- Портал обучения
- Реальные СЗИ

эмулируем хакеров

киберполигон





ЭТАП 5. НЕЗАВИСИМАЯ ОЦЕНКА УСТОЙЧИВОСТИ



✦ Методики проведения испытаний,
эксперты и исследователи.

Выход на bug bounty

Кибериспытания

Лаборатория цифровых двойников

BUG BOUNTY

Платформа для поиска уязвимостей и путей реализации недопустимых событий. Хакеры тренируют навыки и зарабатывают реальные деньги, а компании развивают киберустойчивость — и все остаются в выигрыше.

[Посмотреть все программы](#)



Positive Technologies

Positive Technologies

0-393 200 Р

Вознаграждение



Азбука вкуса

Азбука вкуса

0-100 000 Р

Вознаграждение



INNOSTAGE



Сайберус