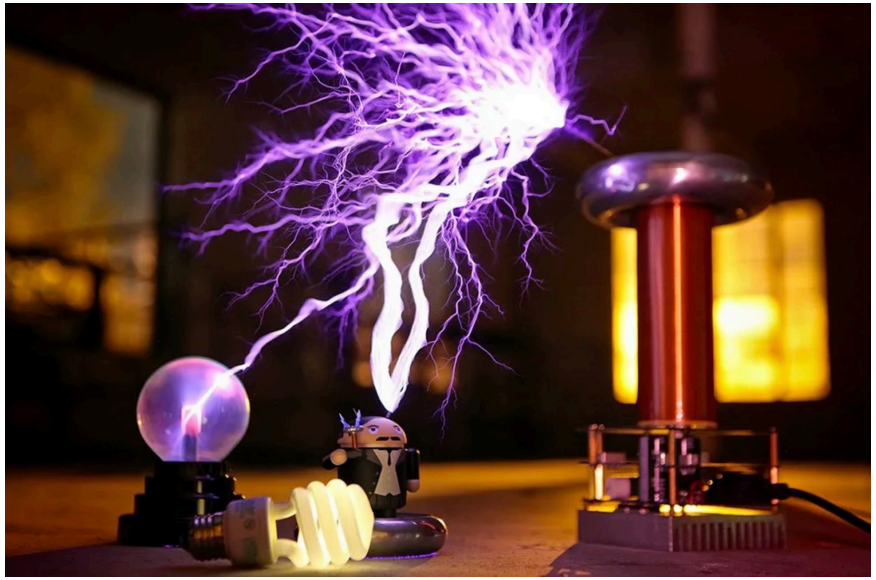
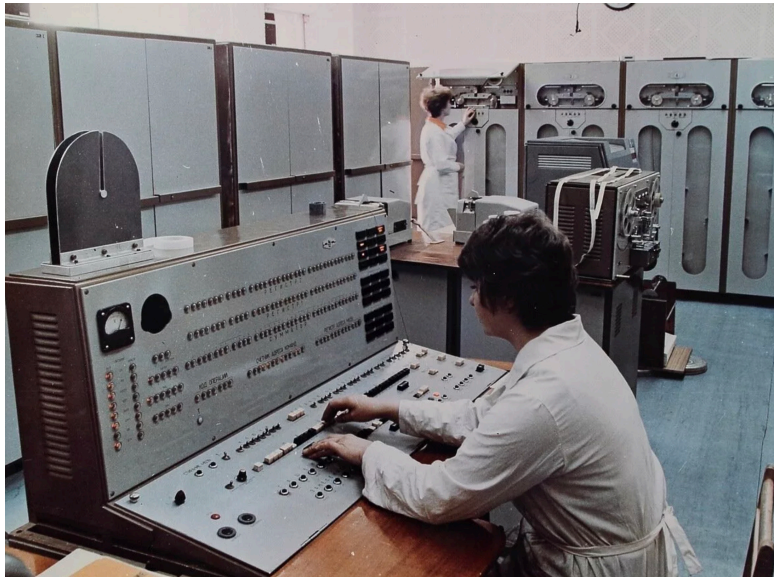
Кибербезопасность в индустриализации 4.0

абсолют банк

Эволюция





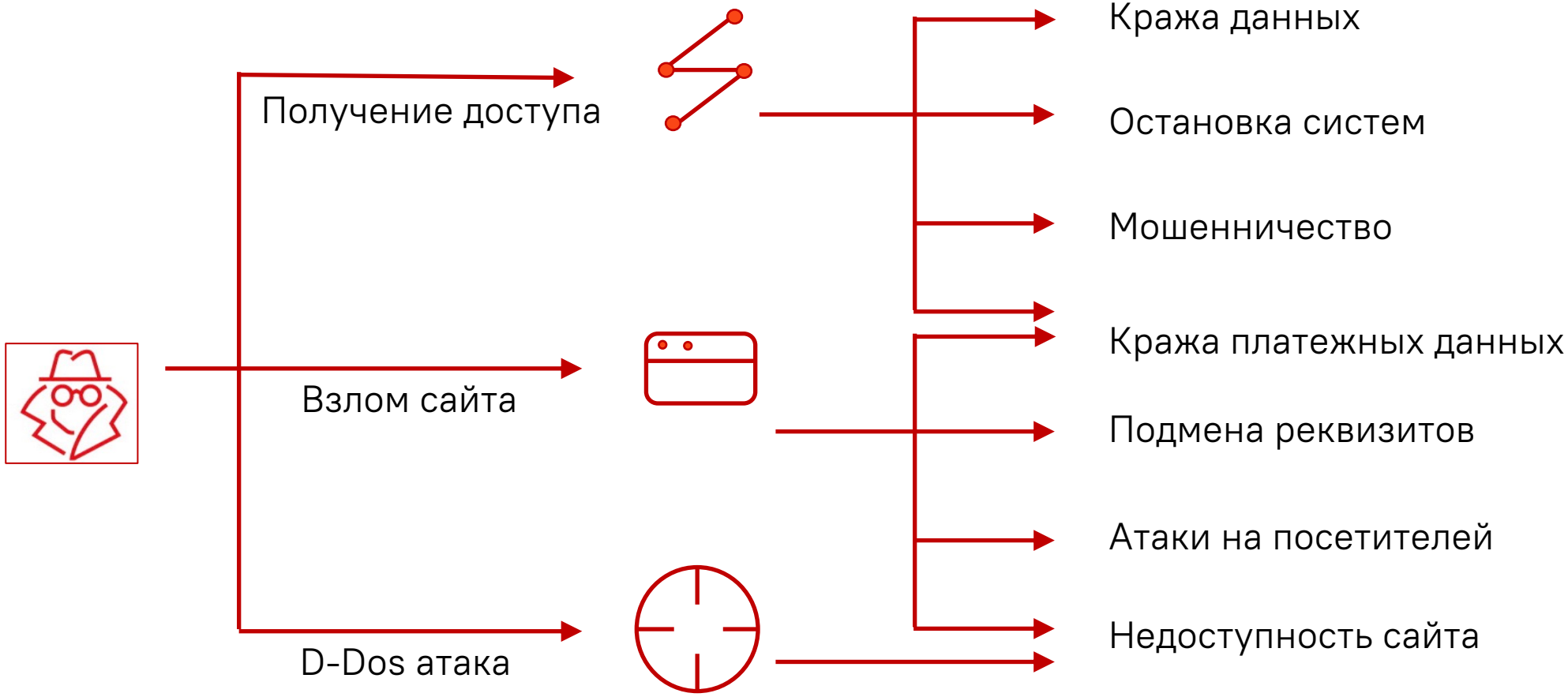

INDUSTRY 4.0
Automation
IOT
System integration
Conection
Big Data
Cloud computing

Аксиома киберпреступности

Завязаны ли ваши процессы на:

- Данных
- Технологиях
- Людях

Недопустимые события



Матрица недопустимых событий

категория	недопустимые события	Злоумышленник	АБС банка	ДБО юр лица	ДБО физ лица	АРМ КБР	Платформа Гарантии	Канал связи
Финансовые потери	вывод д/с с р/с	внешний	получение доступа	получение доступа	получение доступа			
			эксп уязвимости	эксп уязвимости	эксп уязвимости			
		внутренний	мош, инсайдер	мош, инсайдер				
		автоматиз система	вредоносное по	вредоносное по	вредоносное по			
	вывод д/с с к/с	внешний	получение доступа			получение доступа		
			эксп уязвимости			эксп уязвимости		
		внутренний	мош, инсайдер			мош, инсайдер		
		автоматиз система	вредоносное по					
	мошеннические операции	внешний	получение доступа	получение доступа	мош, инсайдер	мош, инсайдер	получение доступа	получение доступа
		внутренний	мош, инсайдер	мош, инсайдер		мош, инсайдер	мош, инсайдер	мош, инсайдер
		автоматиз система	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по
	мошеничество в программах	внешний	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости
			недобр поставщик	недобр поставщик	недобр поставщик	недобр поставщик	недобр поставщик	недобр поставщик
		внутренний	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по
		автоматиз система	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по
Прерывание деятельности	остановка работы систем	внешний	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости
			перебои с доступом	перебои с доступом	перебои с доступом	перебои с доступом	перебои с доступом	перебои с доступом
			недобр поставщик	недобр поставщик	недобр поставщик		недобр поставщик	недобр поставщик
		внутренний	ошибка эксплуатации	ошибка эксплуатации	ошибка эксплуатации	ошибка эксплуатации	ошибка эксплуатации	ошибка эксплуатации
			вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по
		автоматиз система	получение доступа	получение доступа	получение доступа	получение доступа	получение доступа	получение доступа
	перебои внутреннего обслуживания	внешний	перебои с доступом	перебои с доступом	перебои с доступом	перебои с доступом	перебои с доступом	перебои с доступом
		внутренний	перебои с доступом	перебои с доступом	перебои с доступом	перебои с доступом	перебои с доступом	перебои с доступом
		автоматиз система	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по
	перебои внешнего обслуживания	внешний	перебои с доступом	перебои с доступом	перебои с доступом		перебои с доступом	перебои с доступом
			недобр поставщик	недобр поставщик	недобр поставщик		недобр поставщик	недобр поставщик
		внутренний	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер
		автоматиз система	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по
	перебои взаимодействия с гос органиами	внешний	недобр поставщик	недобр поставщик	недобр поставщик	недобр поставщик	недобр поставщик	недобр поставщик
		внутренний	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер
		автоматиз система	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по
Искажение или утрата данных	информации в базах	внешний	получение доступа	получение доступа	получение доступа	получение доступа	получение доступа	получение доступа
			эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости
		внутренний	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер
		автоматиз система	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по
	резервные копии	внешний	получение доступа	получение доступа	получение доступа	получение доступа	получение доступа	получение доступа
			эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости
		внутренний	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер
		автоматиз система	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по
	искажение на официальных ресурсах	внешний	получение доступа	получение доступа	получение доступа	получение доступа	получение доступа	получение доступа
			эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости
		внутренний	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер
		автоматиз система	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по
	публикация ложной информации	внешний	получение доступа	получение доступа	получение доступа	получение доступа	получение доступа	получение доступа
		внутренний	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер
		автоматиз система	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по
Утечка чувствительных данных	базы данных	внешний	получение доступа	получение доступа	получение доступа	получение доступа	получение доступа	получение доступа
			эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости
		внутренний	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер
		автоматиз система	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по
	документы	внешний	получение доступа	получение доступа	получение доступа	получение доступа	получение доступа	получение доступа
			эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости
		внутренний	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер
		автоматиз система	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по
	доступы к системам	внешний	получение доступа	получение доступа	получение доступа	получение доступа	получение доступа	получение доступа
			эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости
		внутренний	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер
		автоматиз система	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по
	информация об уязвимостях	внешний	получение доступа	получение доступа	получение доступа	получение доступа	получение доступа	получение доступа
			эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости	эксп уязвимости
		внутренний	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер	мош, инсайдер
		автоматиз система	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по	вредоносное по

* что нужно сделать злоумышленнику для реализации недопустимого события

Ключевые действия для реализации недопустимых событий

Внешний злоумышленник:

- получение доступа в сеть банка через логин/пароль
- получение доступа в сеть банка через эксплуатацию уязвимостей
- использование имеющегося доступа для создания недопустимого события (для аутсорсинга и партнеров)
- Распространение вредоносного ПО

Внутренний злоумышленник

- мошеннические действия
- сговор
- саботаж
- распространение вредоносного ПО

Автоматизированные системы

- Распространение вредоносного ПО
- Использование скриптов для анализа инфраструктуры и эксплуатации уязвимостей

Из чего можно сделать вывод о ключевых рисках

- Накапливание уязвимостей приводит к их нежелательной эксплуатации злоумышленником
- Гиперзависимость от общих данных и технологий приводит к излишнему доступу со стороны партнеров, аутсорсинга , а размытый периметр позволяет обойти ограничения
- Благодаря большому кол-ву накопленных уязвимостей, размытому периметру и повышенному интересу к атакам на инфраструктуру банка необходимо обеспечить компетентное противодействие, а также поиск артефактов, которые могут стать причиной атак.

Кибербезопасность в бизнесе

Регулятор

- Соблюдение требований
- Выполнение комплаенса
- Лицензирование отдельных видов деятельности
- Общая стратегия кибербезопасности государства

Риски

- Приемлемые операционные риски
- Резервирование капитала
- Страхование риска
- Отчеты в рейтинговые агентства

Бизнес

- Результативная кибербезопасность
- Новые возможности и развитие
- Конкурентноспособные продукты
- Гибкая бизнес модель

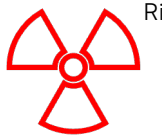
Клиенты

- Доступность сервисов
- Безопасность сервисов
- Защита данных
- Цена продукта

Цифровая эпоха 4.0

683-П
719-П
152-ФЗ

От регулятора



Risk

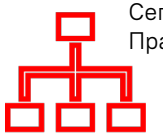
От рисков

ALE
ROSI
NPV
VaR

От бизнеса

Сверхзависимость от цифровых данных	Противостоять современным техникам и тактикам
Трансформация учитывает недопустимые события	Кибербезопасность помогает соблюдать обязательства

Формальный подход

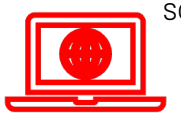


Сегментация
Практика ITSM

От ИТ

Кража данных
Остановка ДБО
Кража денег

От недопустимых событий



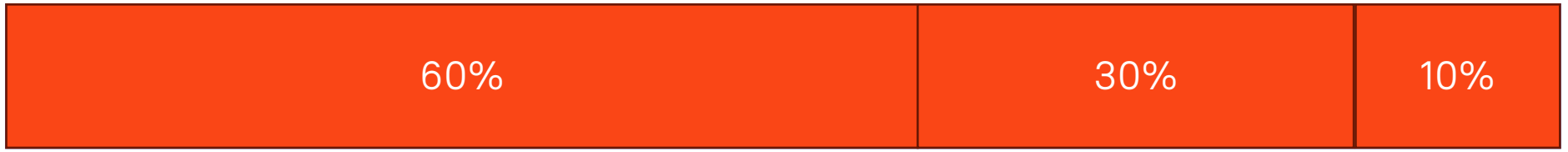
SOC

От реагирования

Стратегия развития

- Сеть кибербезопасности и технологии пограничного доступа
- Защита данных в концепции фабрики данных
- Автоматизация и гипераватоматизация реагирования на инциденты
- Безопасность публичного облака
- Безопасная разработка
- Автоматизация процессов аудита
- Транзакционный и внутренний антифрод

Стоимость продукта



ИТ ИБ Данные

Спасибо

абсолют банк