Автоматизация процессов обработки рисков киберрисков.

Преимущество или необходимость?

SECURITY VISION
УВИДЕТЬ БЕЗОПАСНОСТЬ

ИНТЕЛЛЕКТУАЛЬНАЯ БЕЗОПАСНОСТЬ ГРУППА КОМПАНИЙ

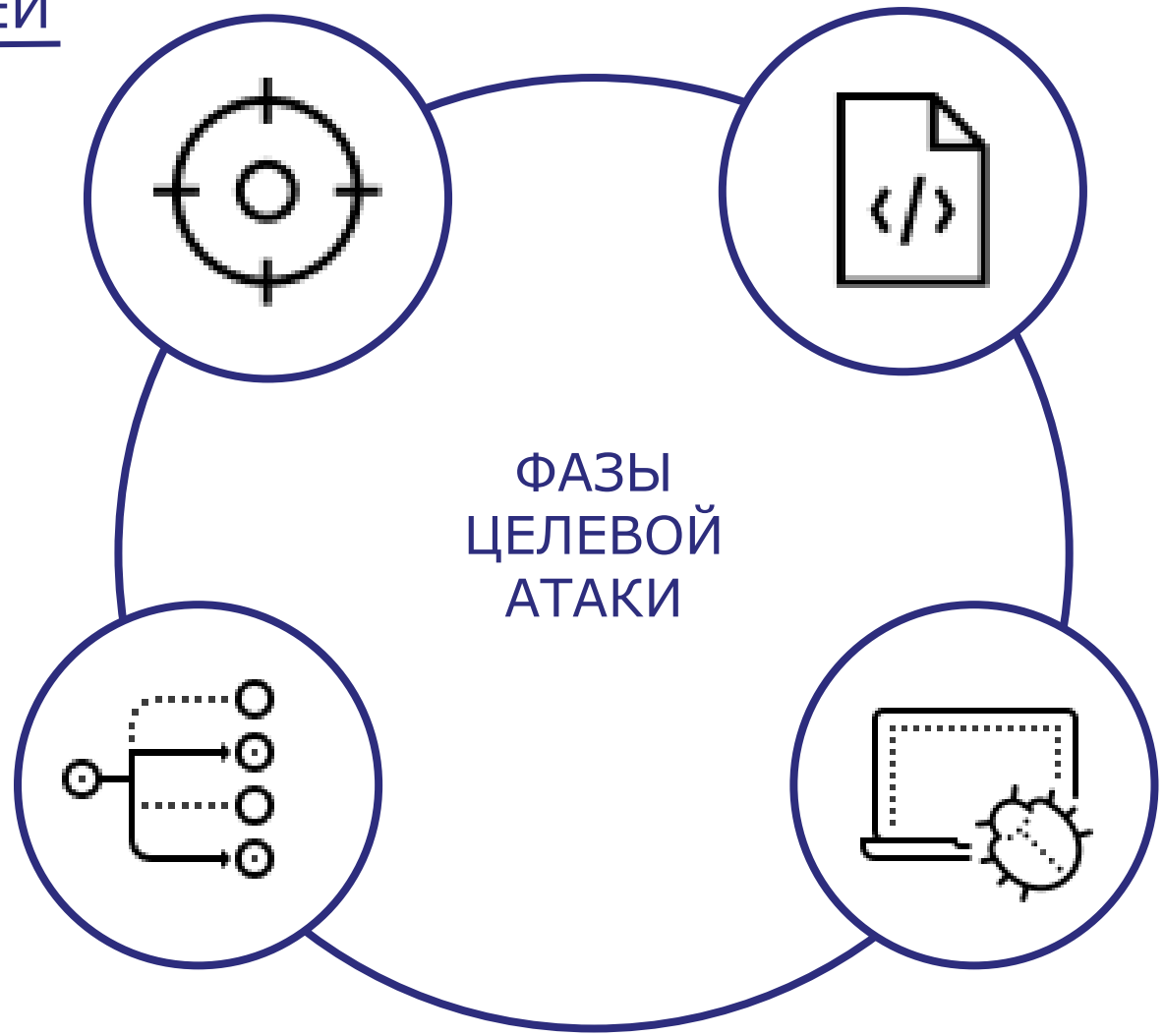
21.11.2018

ДОСТИЖЕНИЕ ЦЕЛЕЙ

- Хищение информации
- Изменение данных
- Влияние на бизнес процесс
- Сокрытие следов

ПОДГОТОВКА

- Выявление цели
- Сбор информации
- Разработка стратегии
- Создание стенда
- Разработка инструментов



РАСПРОСТРАНЕНИЕ

- Закрепление
- Распространение
- Обновление
- Поиск ключевой информации и методов достижения целей

ПРОНИКНОВЕНИЕ

- Техники обхода средств защиты
- Эксплуатация уязвимостей
- Комбинированные техники
- Инвентаризация сети

СХЕМА ВЗАИМОДЕЙСТВИЯ КОМПОНЕНТ

SECURITY VISION CYBER RISK SYSTEM

Автоматизация процессов управления рисками кибербезопасности

INCIDENT RESPONSE SYSTEM

Автоматизация действий по реагированию на инциденты кибербезопасности

СМЕЖНЫЕ СИСТЕМЫ

ПРИМЕРЫ СИСТЕМ:

Системы защиты информации: Межсетевые экраны, Антивирусные средства, Управление инцидентами, Управление доступом к информационным ресурсам, Threat Intelligence, Сканеры безопасности, IPS/IDS системы, DLP системы, Средства контроля доступа

Прикладные системы: Справочники Банка, Почтовая система, Антифрод, Управление операционными рисками, Источники информации об активах, CMDB системы, системы инвентаризации

ТРЕБОВАНИЯ РЕГУЛЯТОРОВ

- ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер.
- Проект Положения Банка России «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»
- Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» (РС БР ИББС-2.2-2009).
- Постановление Правительства РФ от 13.06.2012 N 584 «Об утверждении Положения о защите информации в платежной системе»
- Положение Банка России от 9 июня 2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»
- СТО БР ИББС-1.0-2014
- PCI DSS (version 3.2.1)

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

Интеграции со смежными системами в рамках управления рисками кибербезопасности:
- Анализ информации об уязвимостях кибербезопасности;
- Анализ информации об инцидентах кибербезопасности;
- Анализ информации смежных систем Банка.

Адаптация методологии оценки рисков в соответствии с требованиями бизнеса и регуляторов

Автоматизация отчётности:
- Формирование отчетности по рискам кибербезопасности;
- Визуализация отчетности по рискам кибербезопасности.

Экспресс-оценки риска кибербезопасности внешними экспертами

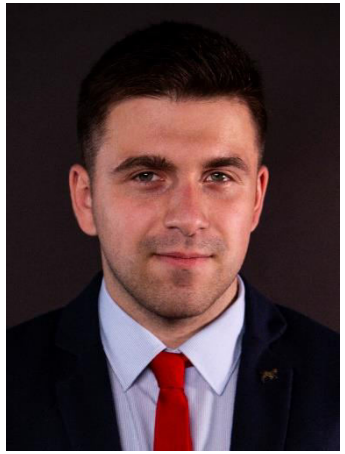
Автоматизация соответствия проекту положения Банка России «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» и другим нормативным актам финансовых учреждений.

Автоматизация взаимодействия с системой:
- Определение области оценки риска кибербезопасности;
- Разработка частной модели угроз;
- Формирование опросных листов;
- Оценка риска кибербезопасности;
- Разработка планов обработки риска кибербезопасности;
- Разработка ключевых индикаторов риска кибербезопасности;
- Оценка рисков кибербезопасности третьих сторон.

Автоматизация аналитических операций:
- Идентификация риска кибербезопасности;
- Анализ информации о мерах защиты;
- Расчет качественных и количественных показателей уровня риска;
- Ведение реестра рисков кибербезопасности;
- Моделирование возможных исходов риска кибербезопасности;
- Мониторинг и контроль уровня риска кибербезопасности.

АНАЛИЗ ЗАТРАТ ПО ГОДАМ

Контакты



Егор Ефремов

Аналитик

eefremov@trimetr.ru

M: +7 (977) 974 83 39

www.securityvision.ru

О компании «Интеллектуальная безопасность»

Компания Интеллектуальная безопасность специализируется в области разработки и внедрения инновационного программного обеспечения по управлению информационной безопасностью. Все технические решения компании Интеллектуальная безопасность основаны на новейших достижениях в области сетевых, компьютерных и коммуникационных технологий и используют оборудование и программное обеспечение производства ведущих компаний.

Компания Интеллектуальная безопасность использует индивидуальный подход, учитывая отраслевую специфику работы Заказчика.
Компания Интеллектуальная безопасность использует комплексный подход, оценивая состояние информационной безопасности Заказчика и защищенность активов компании со всех сторон: Организационную составляющую; Физическую/техническую безопасность; Комплексную информационную безопасность.

Настоящее сообщение содержит информацию только общего характера. При этом ни компания Интеллектуальная безопасность, ни входящие в нее юридические лица, ни их аффилированные лица (далее — «группа «Интеллектуальная безопасность») не представляют посредством данного сообщения каких-либо консультаций или услуг профессионального характера. Ни одно из юридических лиц, входящих в группу «Интеллектуальная безопасность», не несет ответственности за какие-либо убытки, понесенные любым лицом, использующим настоящее сообщение.

ИНТЕЛЛЕКТУАЛЬНАЯ БЕЗОПАСНОСТЬ ГРУППА КОМПАНИЙ