ANGARA SECURITY

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БАНКАХ: НА ЧТО СЕГОДНЯ СТОИТ ОБРАТИТЬ ВНИМАНИЕ

АРБ Ассоциация Российских Банков

NBJ НАЦИОНАЛЬНЫЙ БАНКОВСКИЙ ЖУРНАЛ

ANGARA SECURITY

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТ В БАНКАХ В РАЗРЕЗЕ РЕГУЛЯТОРНЫХ ТРЕБОВАНИЙ

Александр Хонин

Руководитель отдела
консалтинга и аудита
Angara Security

ОСНОВНЫЕ ТРЕБОВАНИЯ ПО ИБ

- 683-П
- 821-П
- 802-П
- ГОСТ 57580.1
- ГОСТ 57580.2

- 716-П
- 787-П
- ГОСТ 57580.3
- ГОСТ 57580.4

- 152-ФЗ
- Приказ 21
- ПП-1119
- Приказ 378
- Приказ 77
- Приказы РКН

- 187-ФЗ
- ПП-127
- Приказ 235
- Приказ 236
- Приказ 239

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Процессы обработки ПДн

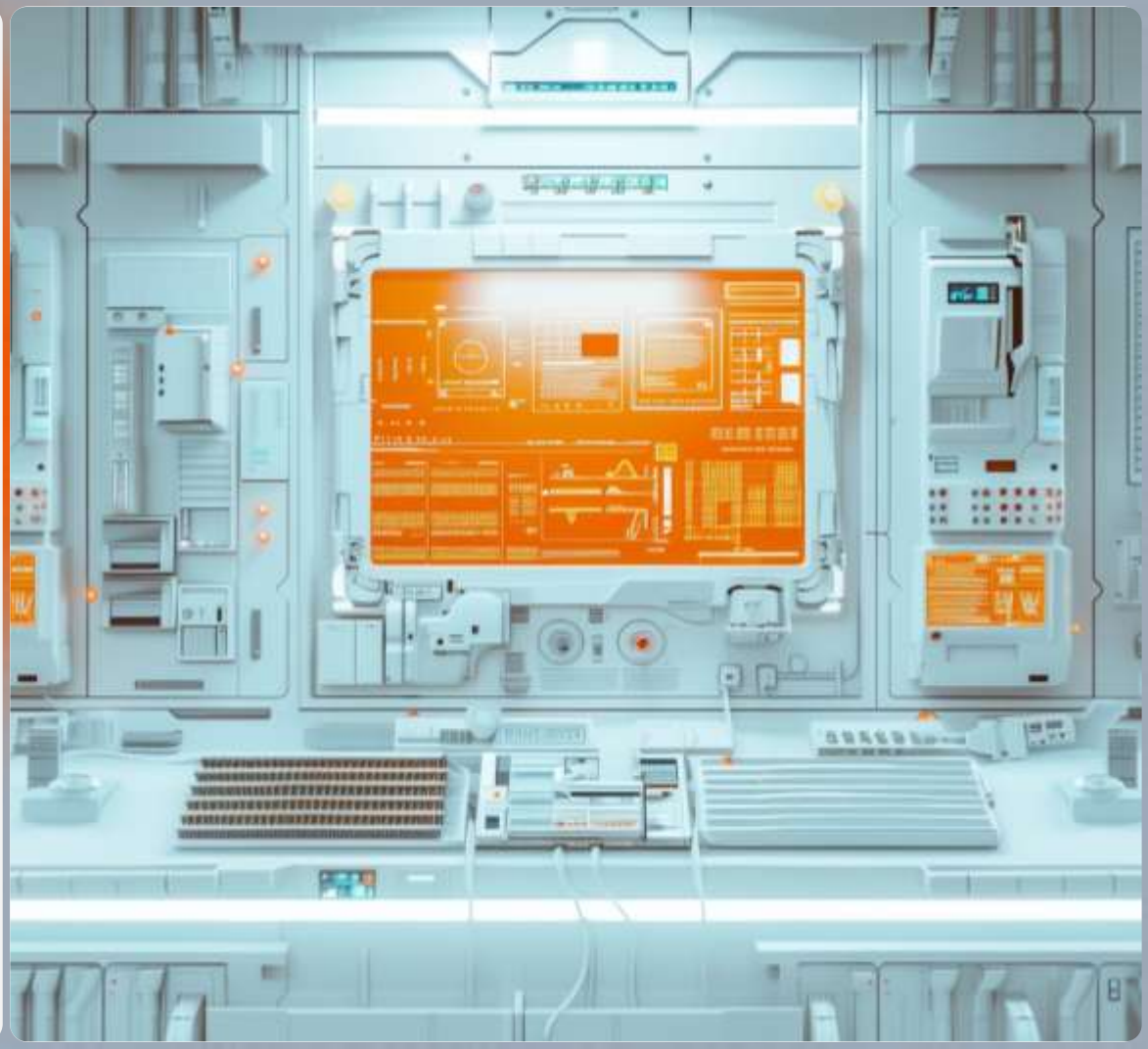
- Соответствие процессов обработки ПДн требованиям законодательства
- Организационно-распорядительная документация в части обработки ПДн

Процессы защиты ПДн

- Система защиты ПДн
- Взаимодействие с ГосСОПКА и РКН

НА ЧТО НЕОБХОДИМО ОБРАТИТЬ ВНИМАНИЕ

- Вопросы обработки ПДн (изменения 2022 г.)
- Средства защиты информации
- Модель угроз безопасности информации
- Оценка соответствия



ЗАЩИТА КИИ

Категорирование объектов КИИ

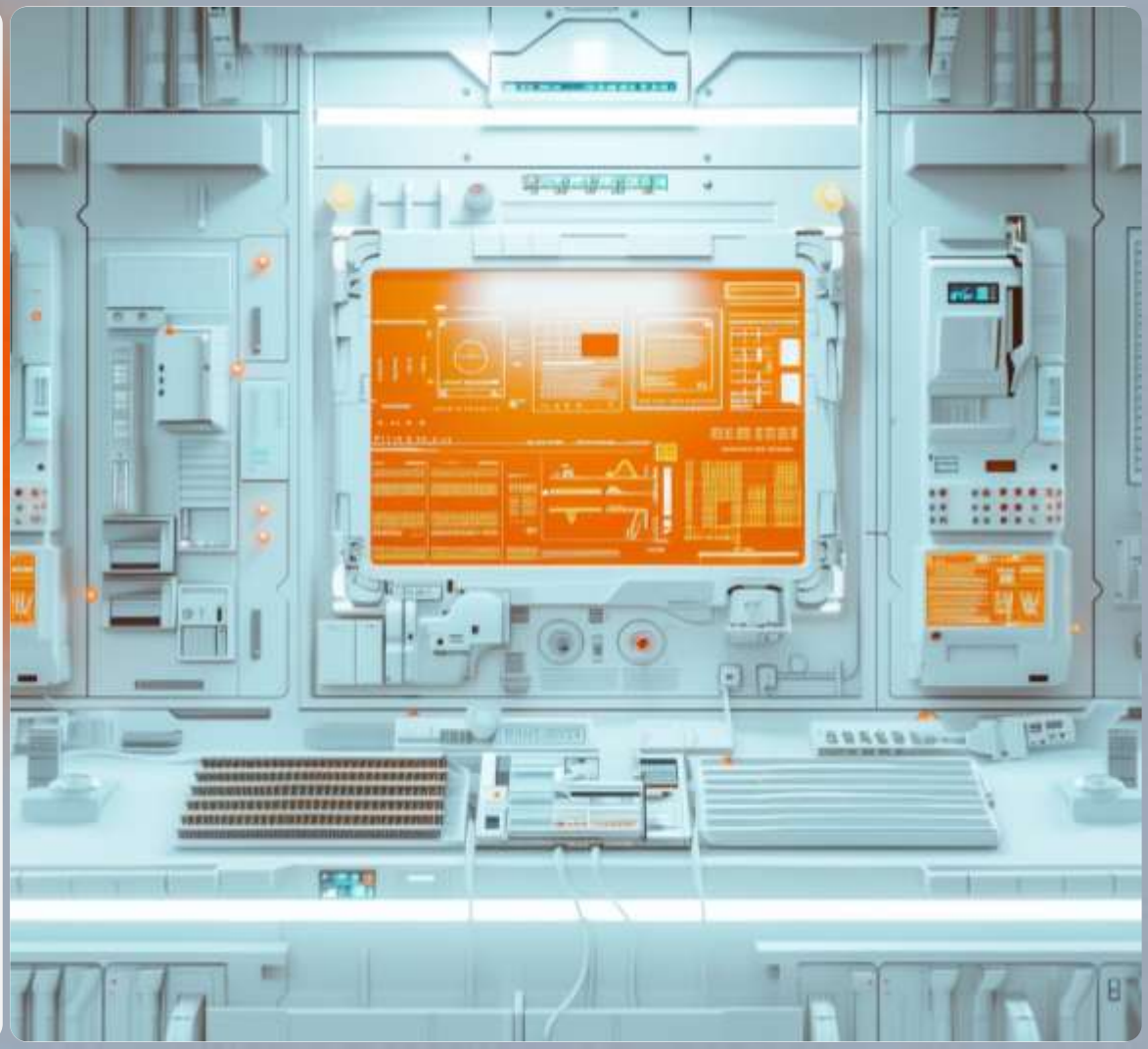
- Определение перечня объектов КИИ
- Определение категорий значимости объектов КИИ

Обеспечение безопасности объектов КИИ

- Система обеспечения безопасности объектов КИИ
- Взаимодействие с ГосСОПКА

НА ЧТО НЕОБХОДИМО ОБРАТИТЬ ВНИМАНИЕ

- Выделение объектов КИИ
- Обоснование по показателям критериев значимости
- Периодический пересмотр результатов категорирования
- Указ Президента РФ от 1 мая 2022 № 250



ПОЛОЖЕНИЯ БАНКА РОССИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

- **Положение Банка России от 17.04.2019 № 683-П**
  «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента»

- **Положение Банка России от 17.08.2023 N 821-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»

- **Положение Банка России от 25.07.2022 № 802-П**
  «О требованиях к защите информации в платежной системе Банка России»

Требования по защите информации

- Технологические меры
- Безопасность программного обеспечения
- Тестирование на проникновение и анализ уязвимостей ИБ
- Соответствие требованиям по ИБ

Рекомендации 12-МР

- Оценка выполнения требований Положений

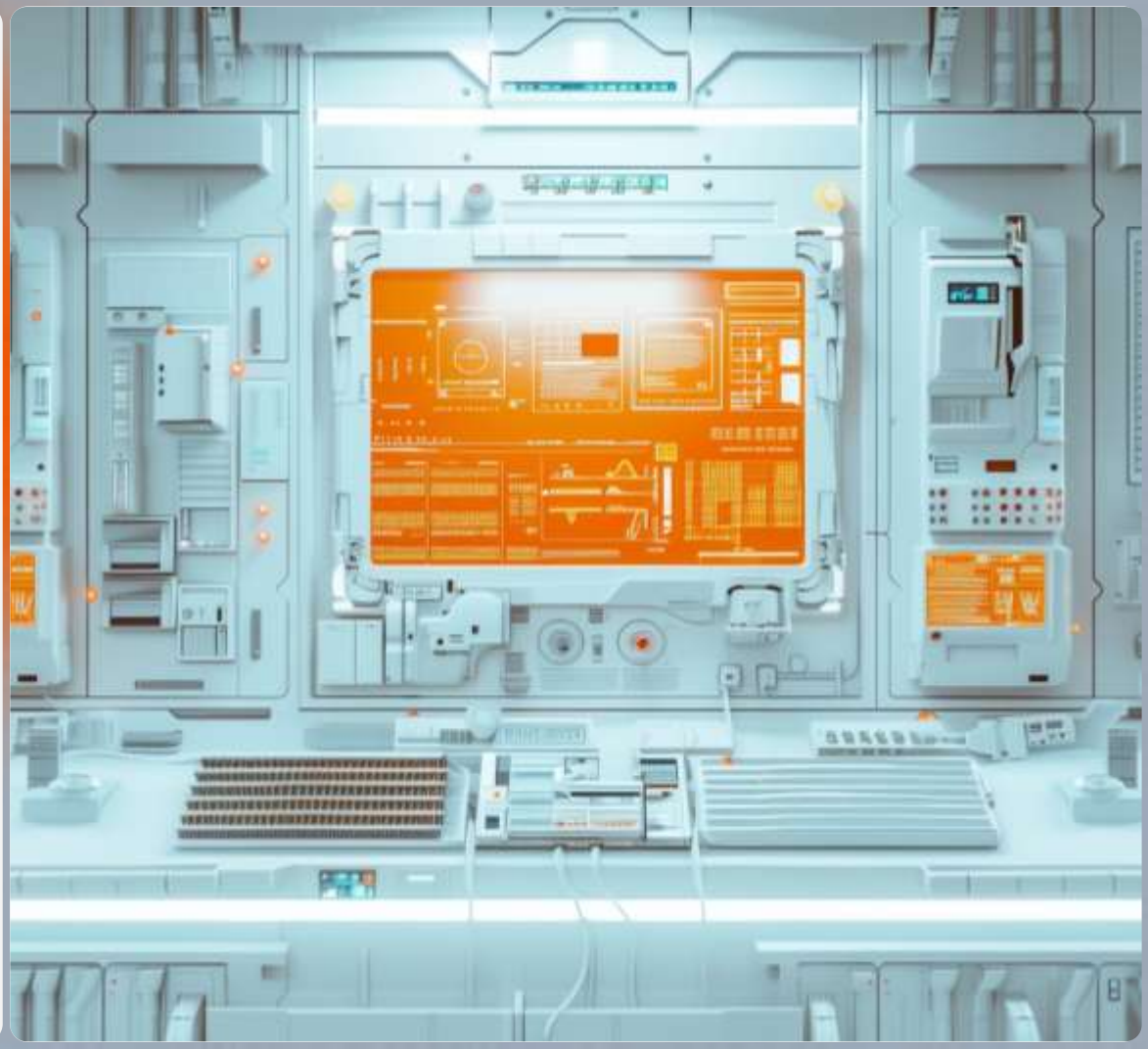
ПОЛОЖЕНИЯ БАНКА РОССИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ

ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый набор организационных и технических мер»

ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия»

НА ЧТО НЕОБХОДИМО ОБРАТИТЬ ВНИМАНИЕ

- Требования по ЗИ из Положений
- Сбор исходных данных и свидетельств
- Выбор мер защиты информации
- Интерпретация требований по ИБ
- Отчетная документация
- Заполнение формы по ОКУД 0409071



ПОЛОЖЕНИЯ БАНКА РОССИИ ПО ОПЕРАЦИОННЫМ РИСКАМ И ОПЕРНАДЕЖНОСТИ

Положение от 08.04.2020 N 716-П

«О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

Положение от 12.01.2022 N 787-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»

ГОСТ Р 57580.3-2022
«Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения»

ГОСТ Р 57580.4-2022
«Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер»

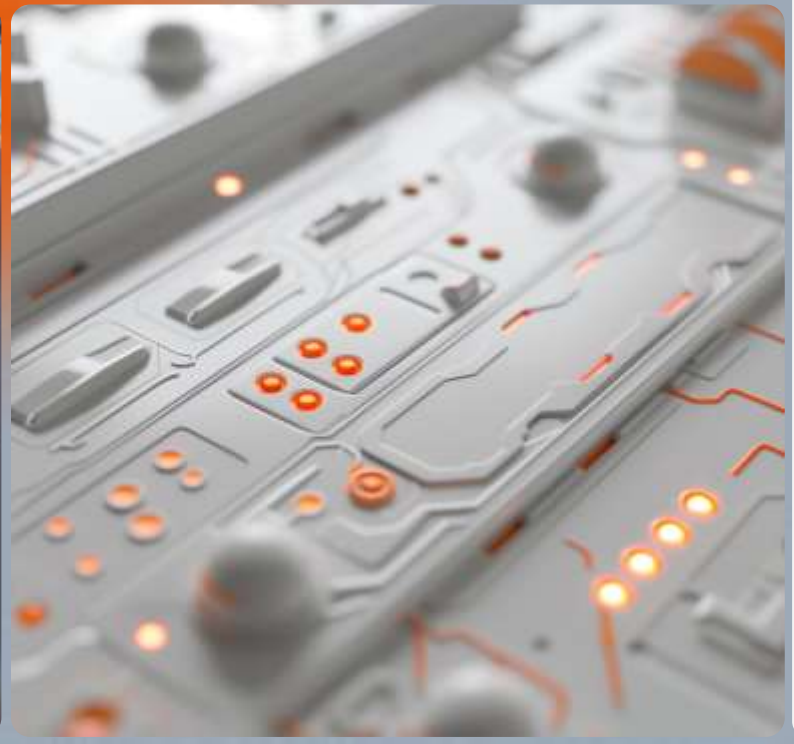
Методические рекомендации по управлению риском информационной безопасности и обеспечению операционной надежности» от 21.03.2024 № 7-МР

МЕЖДУНАРОДНЫЕ ТРЕБОВАНИЯ ПО ИБ

SWIFT Customer Security Policy (Политика безопасности пользователей SWIFT)

SWIFT Customer Security Controls Framework (Концепция обеспечения безопасности пользователей SWIFT)

Требования стандарта PCI DSS



ANGARA SECURITY

ASM

Изучение поверхности атаки
как начало пути к безопасности

Максим Ежов

Руководитель отдела непрерывного
мониторинга безопасности Angara Security

ПОВЕРХНОСТЬ АТАКИ

Каждый сотрудник информационной безопасности в компании должен знать все вверенные ему объекты защиты.

И так как для каждого объекта существует множество векторов атак, совокупность их складывается в термин «поверхность атаки».

*Вектор атаки — последовательность действий или средство для получения неавторизованного доступа к защищенной информационной системе.

АТАКИ = УЯЗВИМОСТИ

Уязвимость — недостаток в системе, используя который можно намеренно нарушить ее целостность и вызвать неправильную (непредсказуемую) работу, в том числе получить неавторизованный доступ к системе.

АТАКИ = УЯЗВИМОСТИ

очень много уязвимостей

28 298

записей было опубликовано в 2023 году в базе уязвимостей Common Vulnerabilities and Exposures (CVE)

8 181

записей в 2023 году было опубликовано в БДУ ФСТЭК

14 748

записей было опубликовано в 2024 году в базе уязвимостей Common Vulnerabilities and Exposures (CVE)

4 807

записей в 2024 году было опубликовано в БДУ ФСТЭК

УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ

Нивелировать количество векторов атак можно путем построения процесса управления уязвимостями — Vulnerability management (VM)

УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ — ЭТО СЛОЖНО

Для грамотного процесса VM необходимо учесть выполнение следующих задач:

- Высоко периодичная инвентаризация инфраструктуры с применением множества инструментов для нивелирования появления активов вне задокументированной информации
- Категоризация и приоритизация с учетом трендов о реально эксплуатируемых уязвимостях злоумышленниками
- Устранение уязвимости путем применения актуальных патчей обновления ПО, политик безопасности или компенсирующих мер
- Контроль не только самого факта устранения уязвимости, но и качества того, как именно уязвимость была устранена

УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ = ВЗАИМОДЕЙСТВИЕ ИТ И ИБ И/ИЛИ ПОДРЯДЧИКА

Уязвимости есть во многих корпоративных системах, будь то сетевой сегмент, персональные компьютеры или даже принтеры.

При этом самой атакуемой частью организации всегда остается ее внешний сетевой периметр.
Те процессы ИБ, которые отвечают за безопасность внешнего периметра, и называют процессом управления поверхностью атак (англ. ASM — Attack Surface Management).

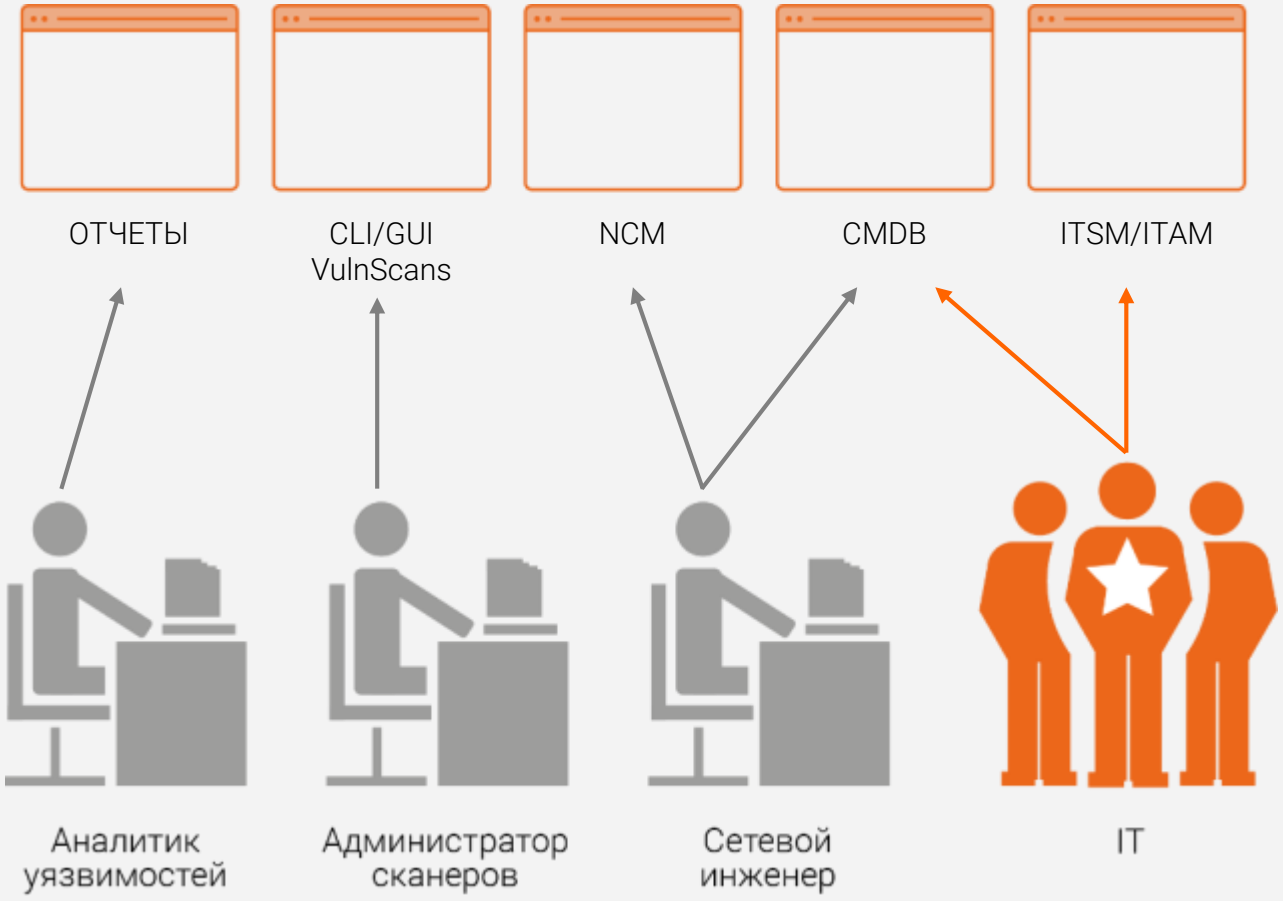
ВАРИАНТЫ РЕАЛИЗАЦИИ ПРОЦЕССА ASM

РЕАЛИЗОВАТЬ ПРОЦЕСС УПРАВЛЕНИЯ ПОВЕРХНОСТЬЮ АТАКИ МОЖНО НЕСКОЛЬКИМИ СПОСОБАМИ:

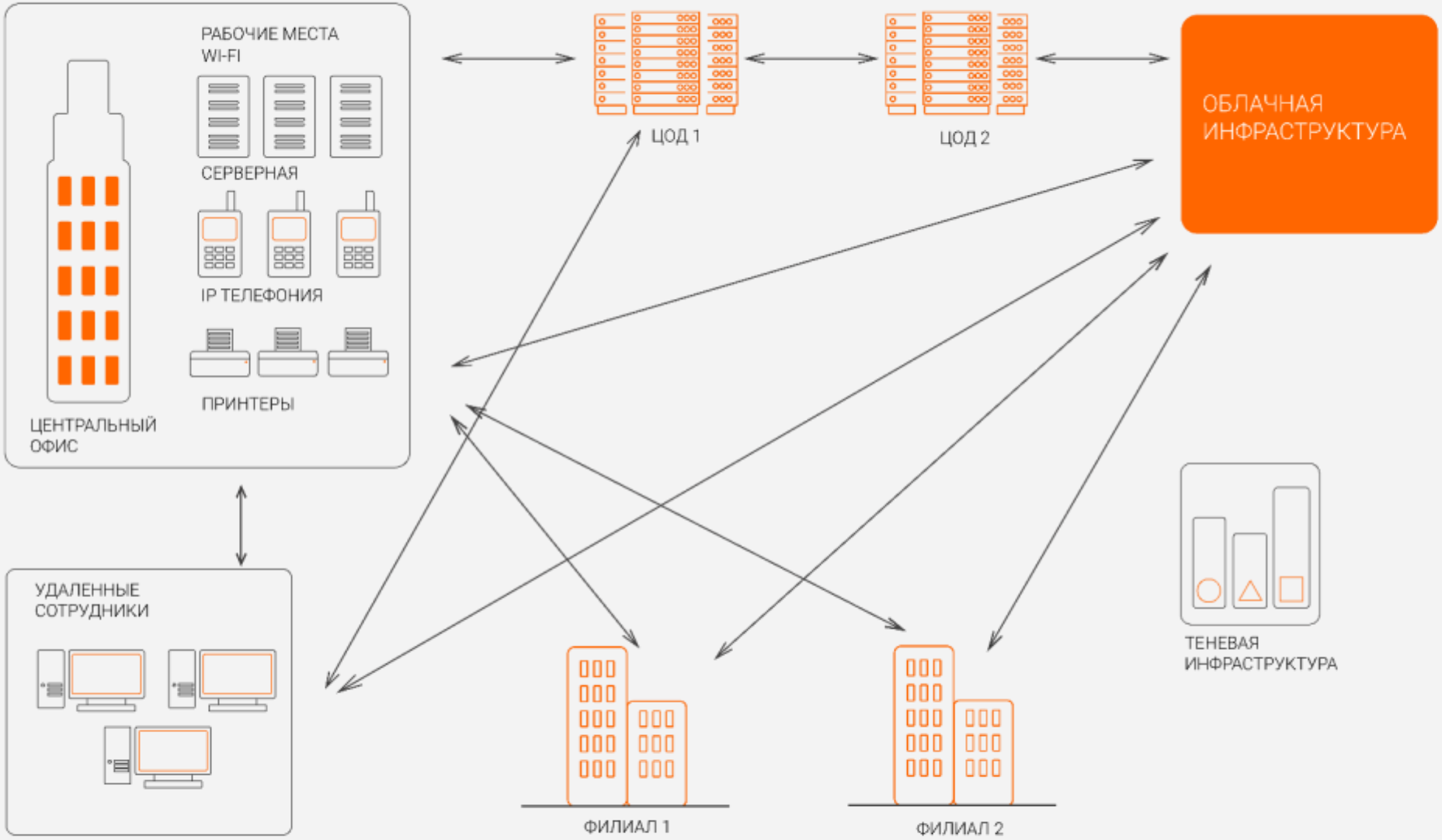
- Силами только специалистов ИБ и ИТ (ручной труд) без применения какого-либо специализированного ПО и только системными средствами
  + специализированное ПО (сетевые сканеры, asset management, сканеры уязвимостей и т.д.)
  + автоматизация взаимодействия используемого ПО (интеграция систем ИБ и ИТ)
  + использование специализированных платформ по ASM, которые агрегируют все результаты со всех сканеров и дают единую консоль управления поверхностью атаки
- Отдать на аутсорсинг

ПОСТРОЕНИЕ РЕШЕНИЯ СВОИМИ СИЛАМИ

ТРЕБУЕТ БОЛЬШОГО КОЛИЧЕСТВА ВЫСТРОЕННЫХ ПРОЦЕССОВ



ПРИМЕР РАСПОЛОЖЕНИЯ АКТИВОВ

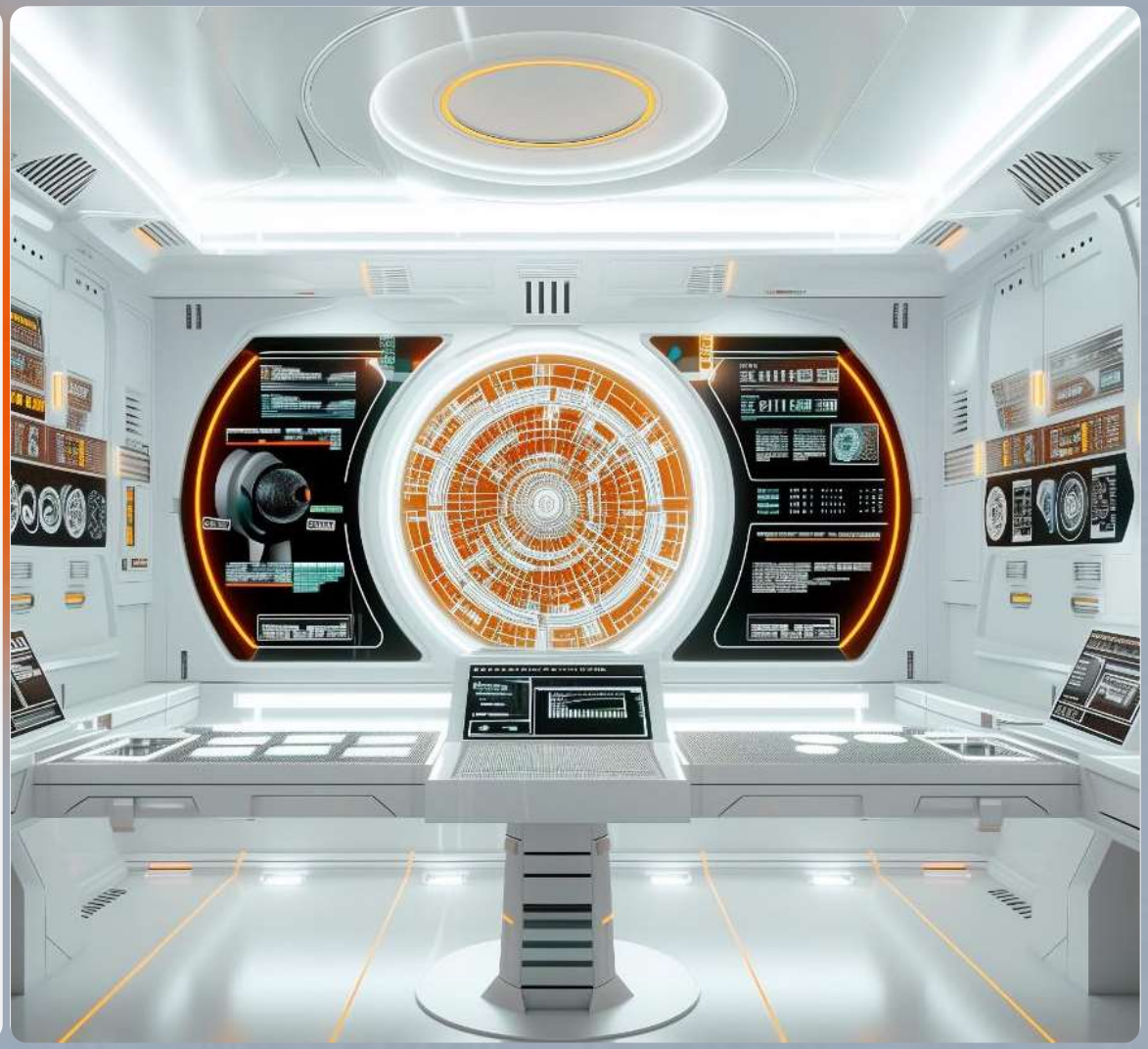


ПРОБЛЕМАТИКА

Сложности вызывает и то, что внешний периметр компании может содержать большое количество информационных систем и сервисов и является самой атакуемой частью корпоративной инфраструктуры, к которой имеют доступ все пользователи сети Интернет.

Публикуются новые сервисы, вводятся в эксплуатацию новые системы, в приложениях появляются новые функции.

Каждое такое изменение несет риск появления небезопасно настроенных систем.



ОТЛИЧИЯ СЕРВИСА ОТ ПРОЦЕССА

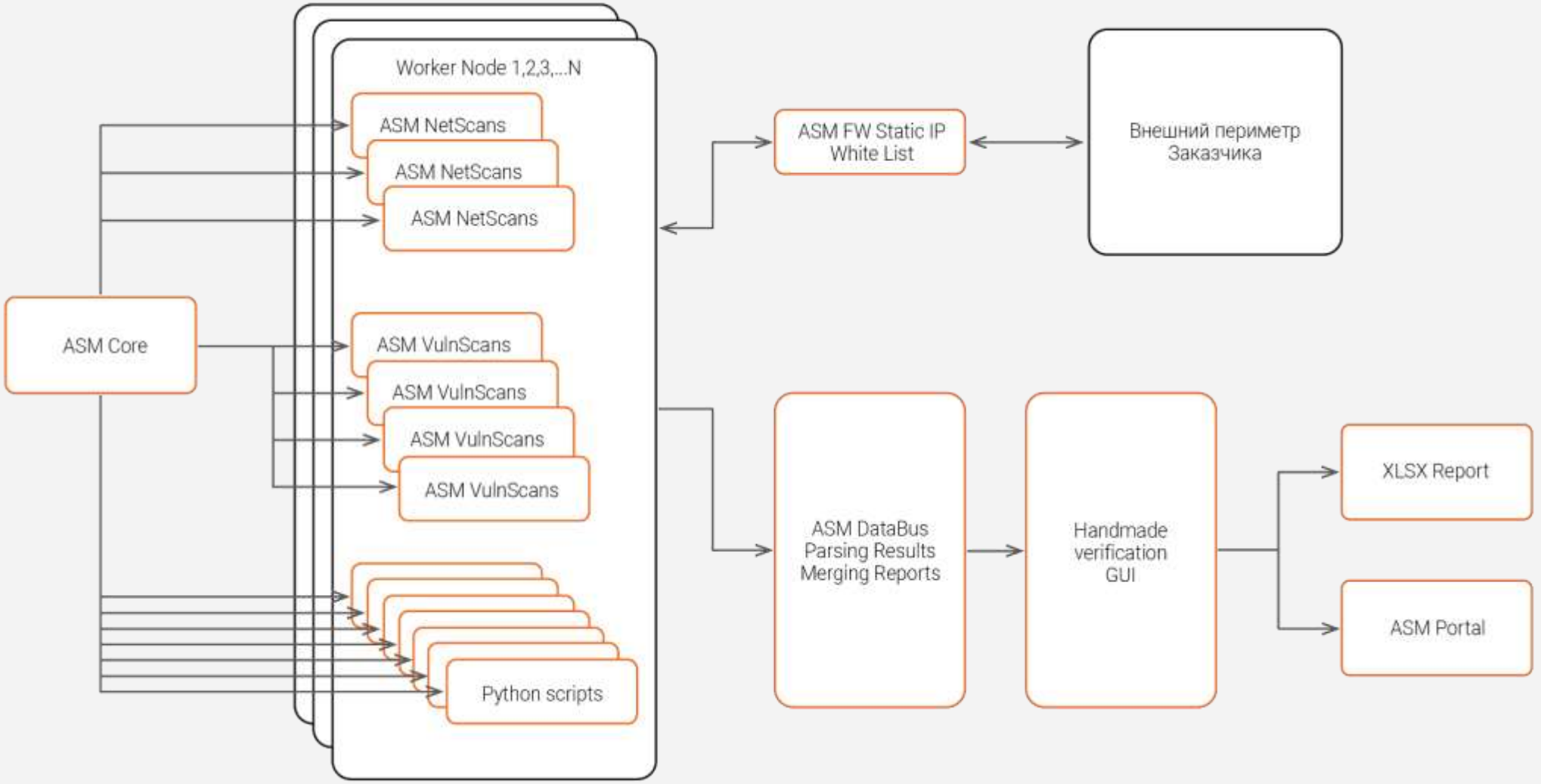
Этапы VM	Работы Этапа	Зоны ответственности	
		При построении своего процесса ASM	При приобретении ASM как сервиса
Инвентаризация	Сканирование сетевых активов	ИТ и ИБ	Подрядчик
	Сканирование веб-приложений	ИТ и ИБ	Подрядчик
	Поиск теневых и незадокументированных активов (via. OSINT)	ИБ	Подрядчик
	Сканирование уязвимостей	ИБ	Подрядчик
Категоризация	Оценка уровня критичности	ИБ	Подрядчик
Приоритизация	На основании трендов мира	ИБ	Подрядчик
	На основании важности актива	ИТ	ИТ
Устранение	Подготовка рекомендаций	ИБ	Подрядчик
	Администрирование ИТ-подсистем	ИТ	ИТ
	Администрирование ИБ-подсистем	ИБ	ИБ
Контроль	Факта устранения	ИБ	Подрядчик
	Качества устранения	ИБ	ИБ

РЕШЕНИЕ ANGARA ASM

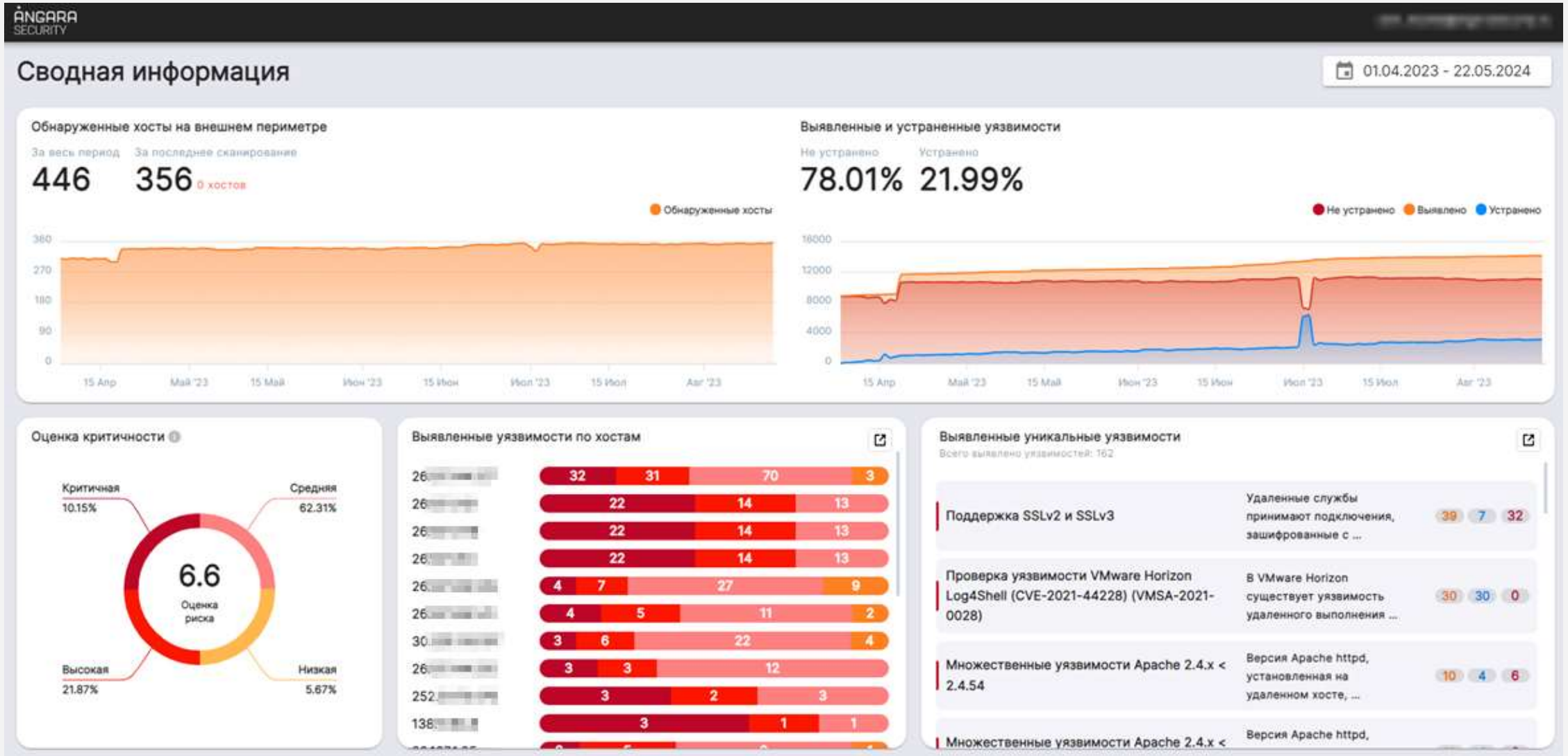
Сервис управления площадью внешних атак

Делегируйте рутинный процесс сканирования внешнего периметра профильным экспертам и освободите ресурсы ИБ-подразделений компании для выполнения других задач

СХЕМА РАБОТЫ СЕРВИСА ANGARA ASM



АГРЕГАЦИЯ ВСЕХ РЕЗУЛЬТАТОВ НА ПОРТАЛЕ



ДЕТАЛИ ТАРИФИКАЦИИ

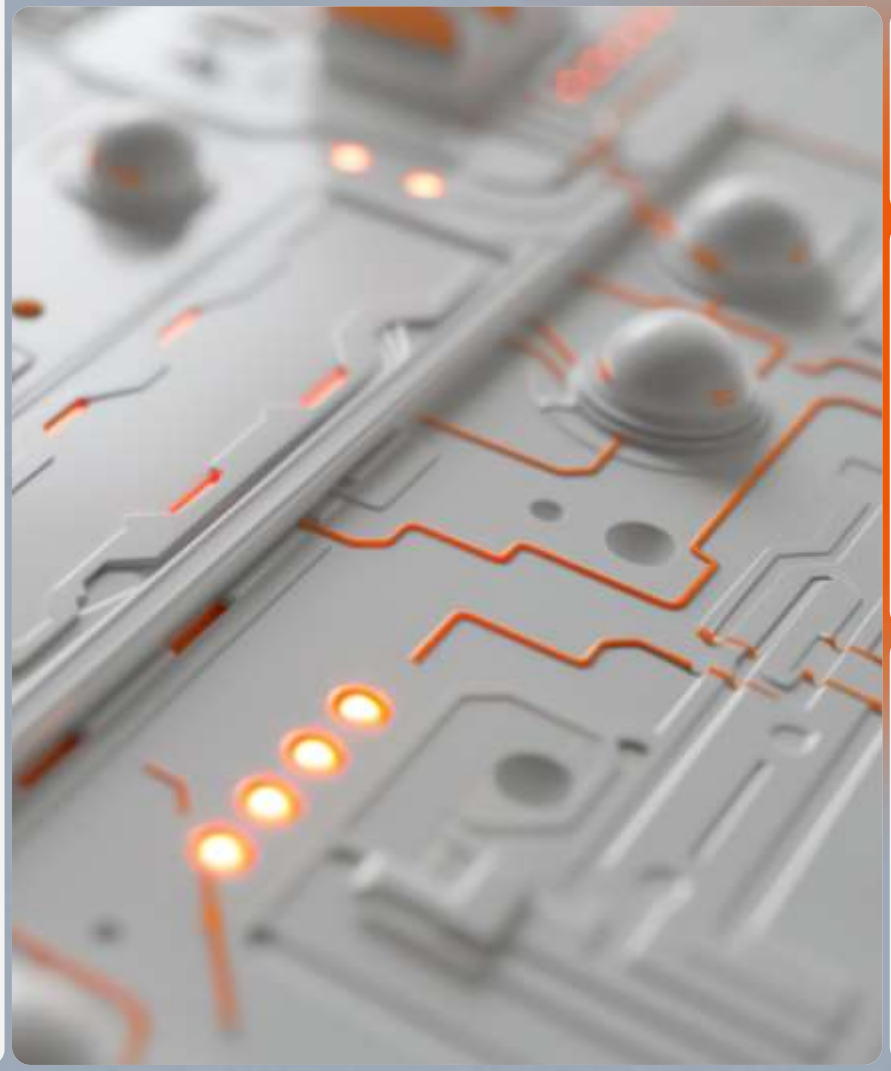
ЛИЦЕНЗИРОВАНИЕ

- По количеству всех сканируемых IP-адресов
- По периодичности инвентаризации активов
- По периодичности сканирования уязвимостей

ДОПОЛНИТЕЛЬНЫЕ ОПЦИИ

- Попытки эксплуатации уязвимостей
- OSINT и защита бренда
- Проверка нестойких паролей
- И многое другое

ПОЧЕМУ СТОИТ ОБРАТИТЬСЯ К НАМ



ASM-ПЛАТФОРМА ОТ КОМПАНИИ ANGARA SECURITY:

- собственная разработка
- портал с визуализацией и ретроанализом
- ручная верификация уязвимостей аналитиками
- рекомендации на русском языке

ВЫГОДА ДЛЯ КОМПАНИИ

Поставленные процессом VM задачи по отношению к внешнему периметру решаются аутсорсинговыми сервисами по управлению площадью атак, носящими одноименное название Attack Surface Management (ASM).
И вот в чем их главная выгода:

Не надо использовать какие бы то ни было on-prem сканеры уязвимостей, тратить ресурсы на их администрирование, сопровождение и размещение

Не надо выделять команду аналитиков уязвимостей для разбора ложноположительных срабатываний и верификации получаемых многостраничных отчетов

Не надо отслеживать все уязвимости, появляющиеся по всему миру

Не надо тратить ресурсы на расчет уровней критичности найденных уязвимостей

Не надо искать, каким именно патчем ПО, политикой безопасности или какими компенсирующими мерами закрывать уязвимость

Не надо отслеживать закрытие уязвимости

СЕРВИС ANGARA ASM СДЕЛАЕТ ВСЕ ЭТО ЗА ВАС

ANGARA SECURITY

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ. ПЕНТЕСТ И ЕГО ВИДЫ

Михаил Сухов

Руководитель отдела анализа защищенности
Angara Security

ВИДЫ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

1. Работы по имитации действий злоумышленника, цель которых – несанкционированное проникновение в информационную систему и получению доступа к конфиденциальной информации. При этих работах нет цели найти все уязвимости.
2. Цель – имитация действий злоумышленника и демонстрация векторов атак, которые возможно реализовать с использованием выявленных уязвимостей.
3. Результат работы – отчет.

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

1. Внешний тест на проникновение:

- Проводится из сети Интернет
- Не требуются дополнительные привилегии (Черный ящик)
- Цель – НСД во внутреннюю сеть ИС

1. Внутренний тест на проникновение:

- Проводится из локальной сети (с присутствием эксперта на площадке) или удаленно (по VPN)
- Требуется только доступ к сетевой розетки (Черный ящик) или минимальная учетная запись (Серый ящик)
- Цель – получение управления ИС или конфиденциальных данных

АНАЛИЗ ЗАЩИЩЕННОСТИ ПРИЛОЖЕНИЙ

Публичные веб и мобильные приложения могут быть не только точкой входа во внутреннюю сеть компании, но и площадкой атаки клиентов этих приложений.

Типовые модели тестирования:

- Черный ящик (нам дается только общедоступная информация)
- Серый ящик (нам даются минимальные привилегии в системе)
- Белый ящик (нам даются множества привилегий и дополнительная внутренняя информация о приложениях)

АНАЛИЗ ЗАЩИЩЕННОСТИ БЕСПРОВОДНЫХ СЕТЕЙ

Беспроводные сети в силу радиуса действия точек доступа вне контролируемого периметра могут стать еще одной точкой входа во внутреннюю сеть.

Оценивается:

- Стойкость используемых данных аутентификации
- Корректность настройки механизмов безопасности (WPA, Radius)
- Возможность проникновения во внутреннюю сеть (изоляция сетевых сегментов)

СОЦИОТЕХНИЧЕСКОЕ ТЕСТИРОВАНИЕ

1. Слабым звеном любой информационной системы является человек.
2. При работах выполняется комплекс действий, целью которых является проверка осведомленности сотрудников об атаках с применением методов социальной инженерии. Разрабатываются различные сценарии и легенды, эксплуатирующие человеческие слабости (любопытство, страх, жажда наживы и т.п.).
3. Варианты сценариев:

- Различные виды почтового фишинга (phishing, spearphishing)
- Телефонный обзвон работников (voice phishing)
- Имитация зараженных носителей

ПРОВЕРКА УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

По нашей статистике **40%** уязвимостей средней и высокой критичности не устраняются корректно.

Причины:

1. Не правильная оценка рисков от найденных уязвимости,
2. Не правильное или неполное исправление уязвимостей,
3. Растянутость сроков исправления уязвимостей,
4. Исправление для галочки.

В рамках перепроверки уязвимостей Исполнитель проверяет была ли уязвимость устранена и можно ли обойти исправление.

ANGARA SECURITY

СПАСИБО ЗА ВНИМАНИЕ!

info@angarasecurity.ru

www.angarasecurity.ru

+7 (495) 269-26-06

121096, г. Москва, ул. Василисы Кожиной, д.1,
к.1 БЦ «Парк Победы»