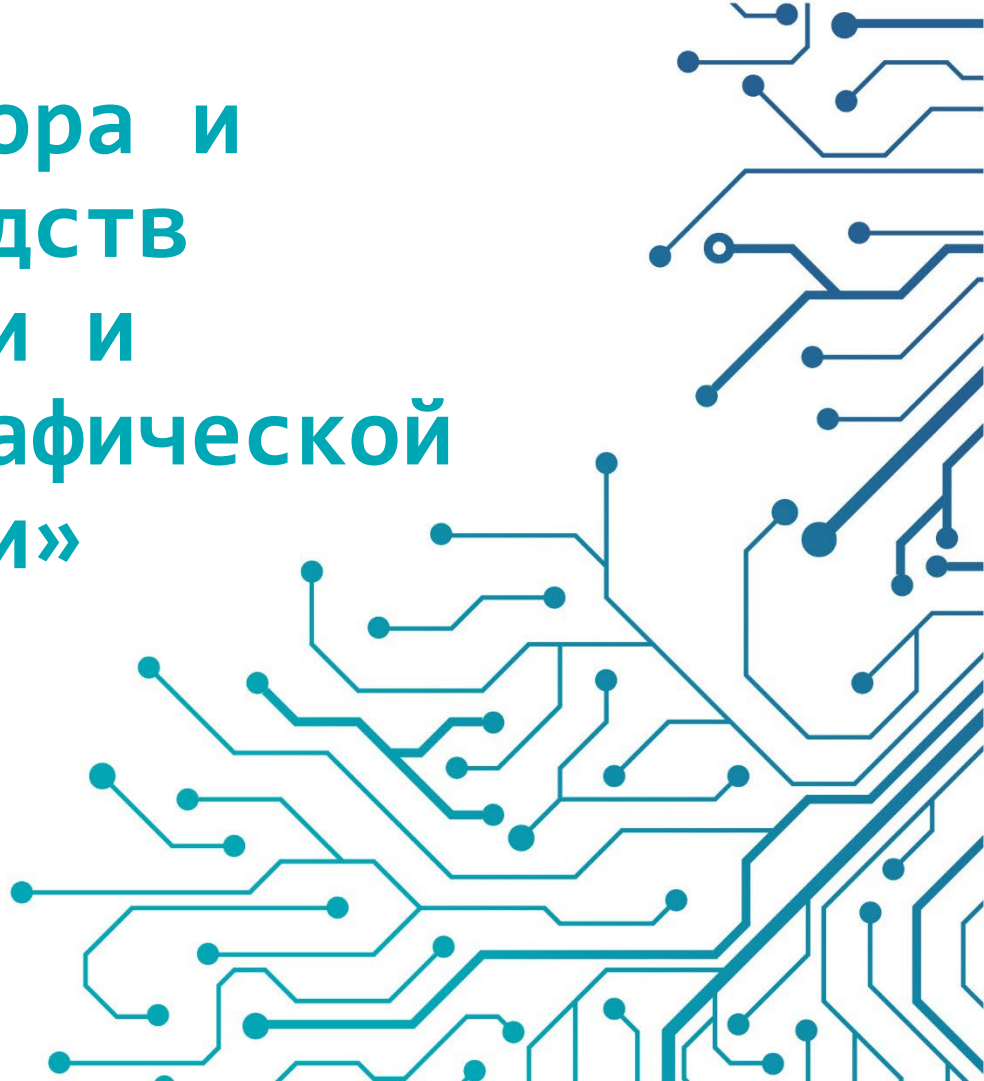
«Особенности выбора и эксплуатации средств защиты информации и средств криптографической защиты информации»

Селифанов Валентин
Заместитель руководителя
обособленного подразделения



infotecs

От чего защищаемся?

От кого защищаемся?

Инсайдеры

Иностранные вендоры, уходящие с рынка и отключающие свои продукты

Хакеры

Как защищаемся?

Растущее количество атак и недоверенных аппаратных компонент

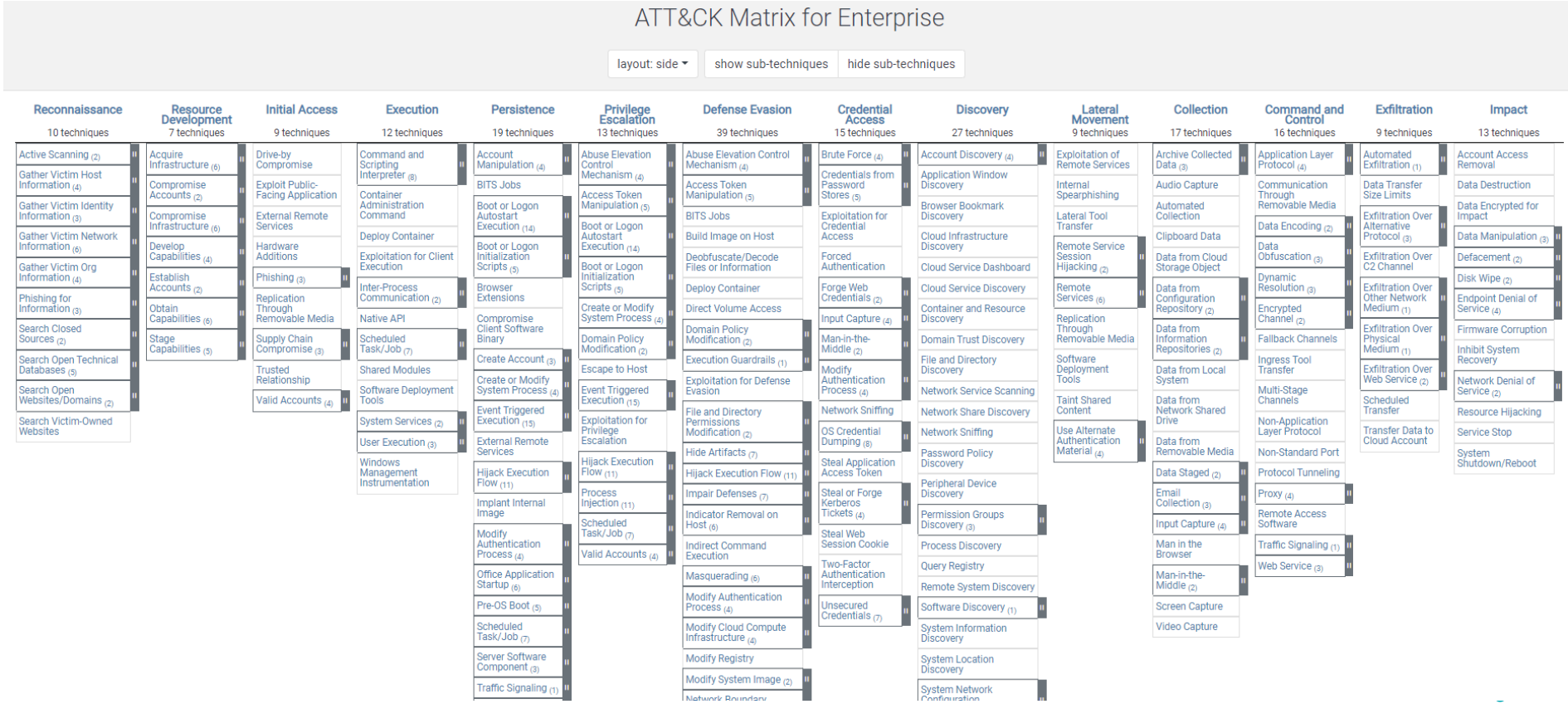
Пользователь – внутренний нарушитель, низкий уровень осведомленности

Удаленная работа, проведение приватных разговоров

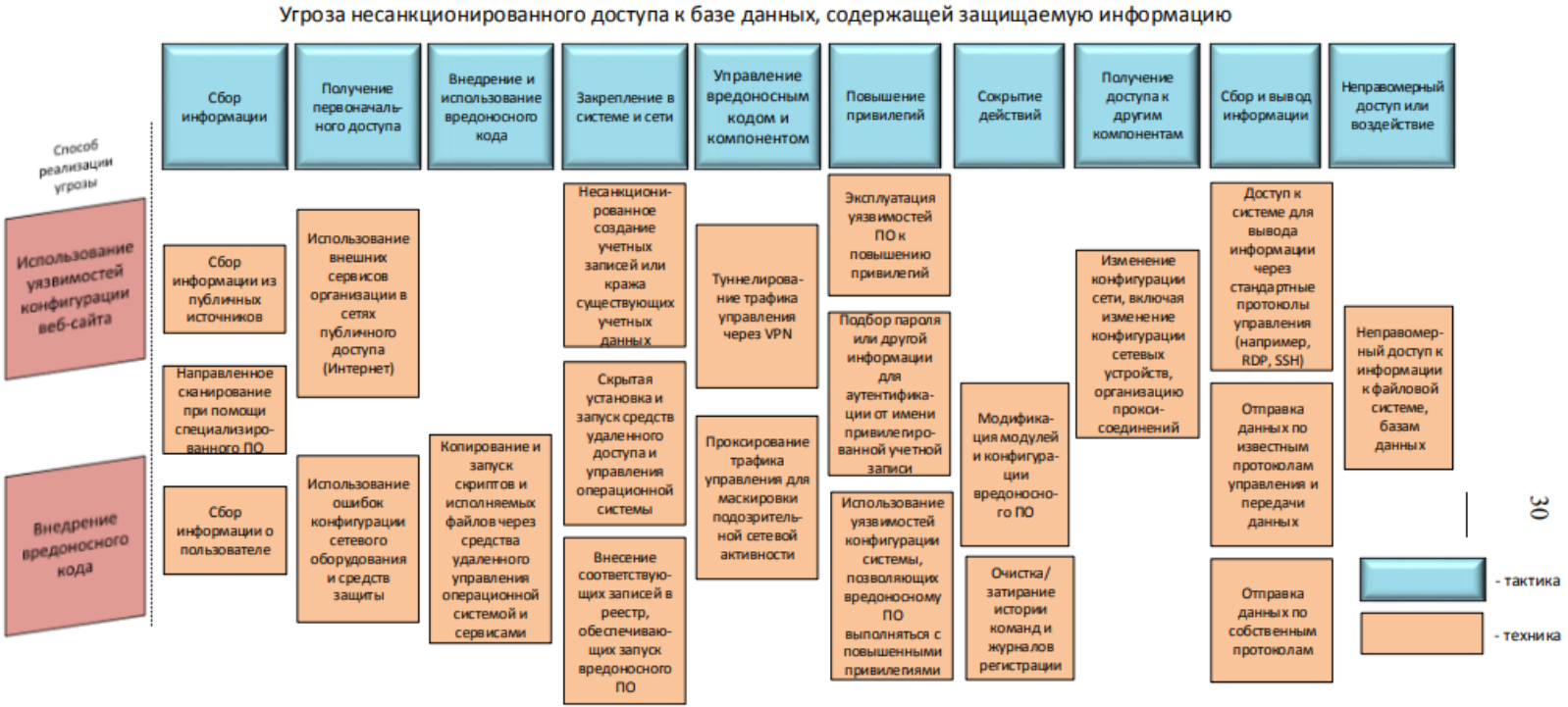
Malware, Ransomeware, Fileless & Never-seen-before attacks

Техники — Тактики — Процедуры

infotecs



«Методика оценки угроз безопасности информации»



Давайте попрактикуемся

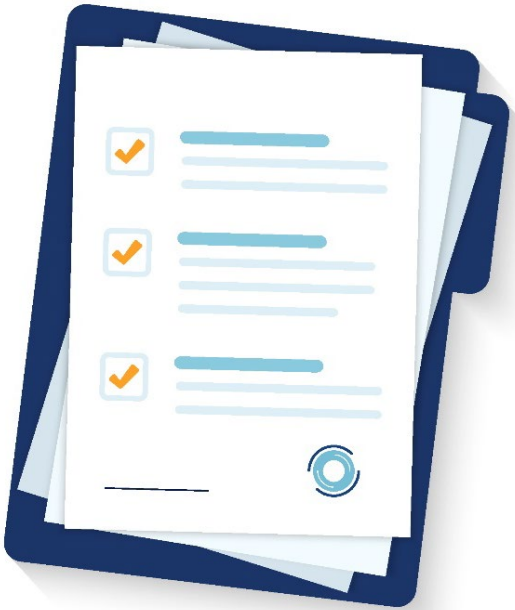
Продукт:

ViPNet EndPoint Protection

Знания:

MITRE ATT&CK

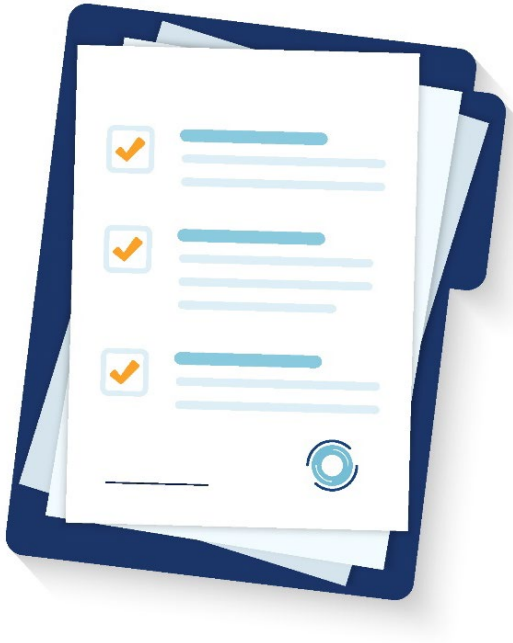
Доверие к операционной системе и пользователю



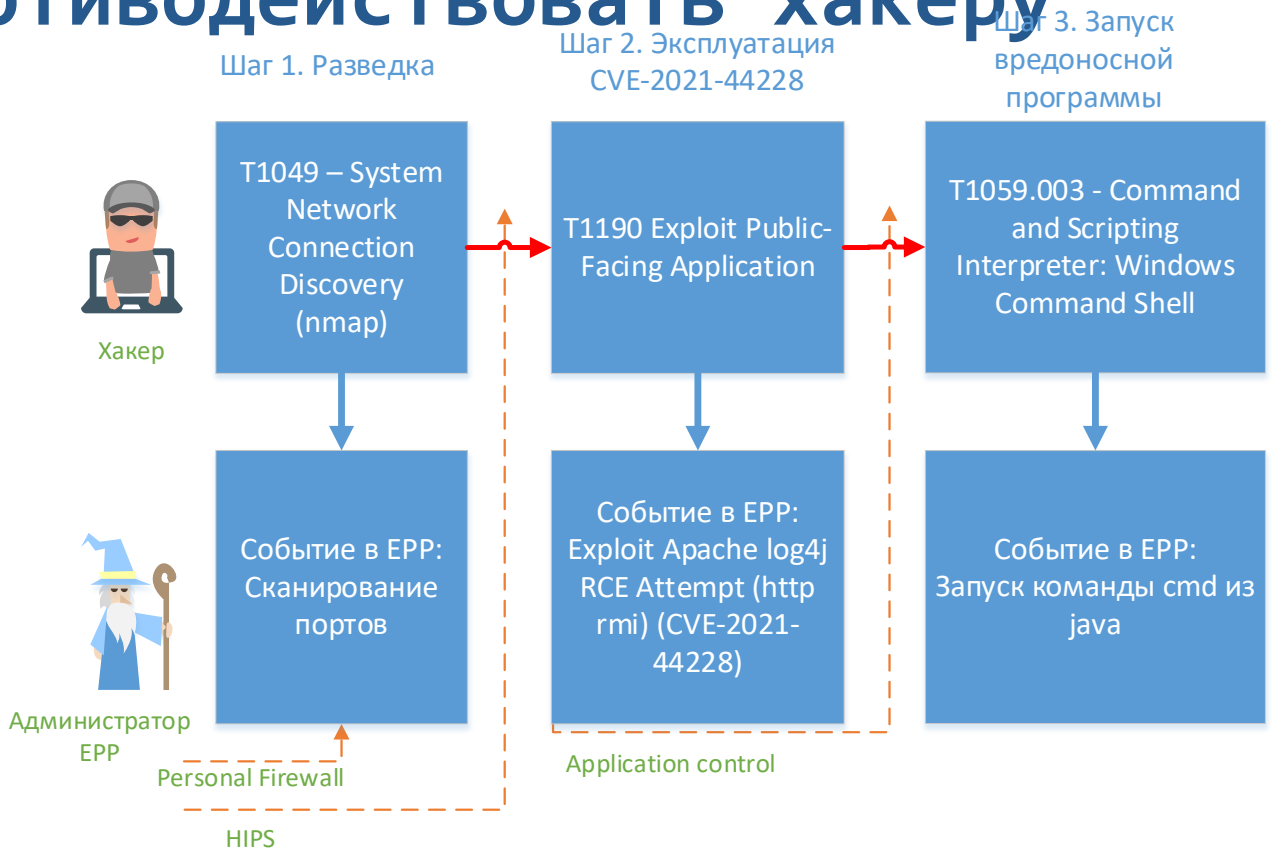
- Каждый пользователь должен работать только в созданном информационном пространстве
- Исключение злонаправленных действий пользователей (хищение данных, с целью передачи третьим лицам)
- Контроль подключения внешних устройств
- Контроль службы обновления ОС и служб обновления иностранного ПО
- Контроль запуска/исполнения новых файлов и приложений из Temp и AppData

Защита от внешних нарушителей и угроз

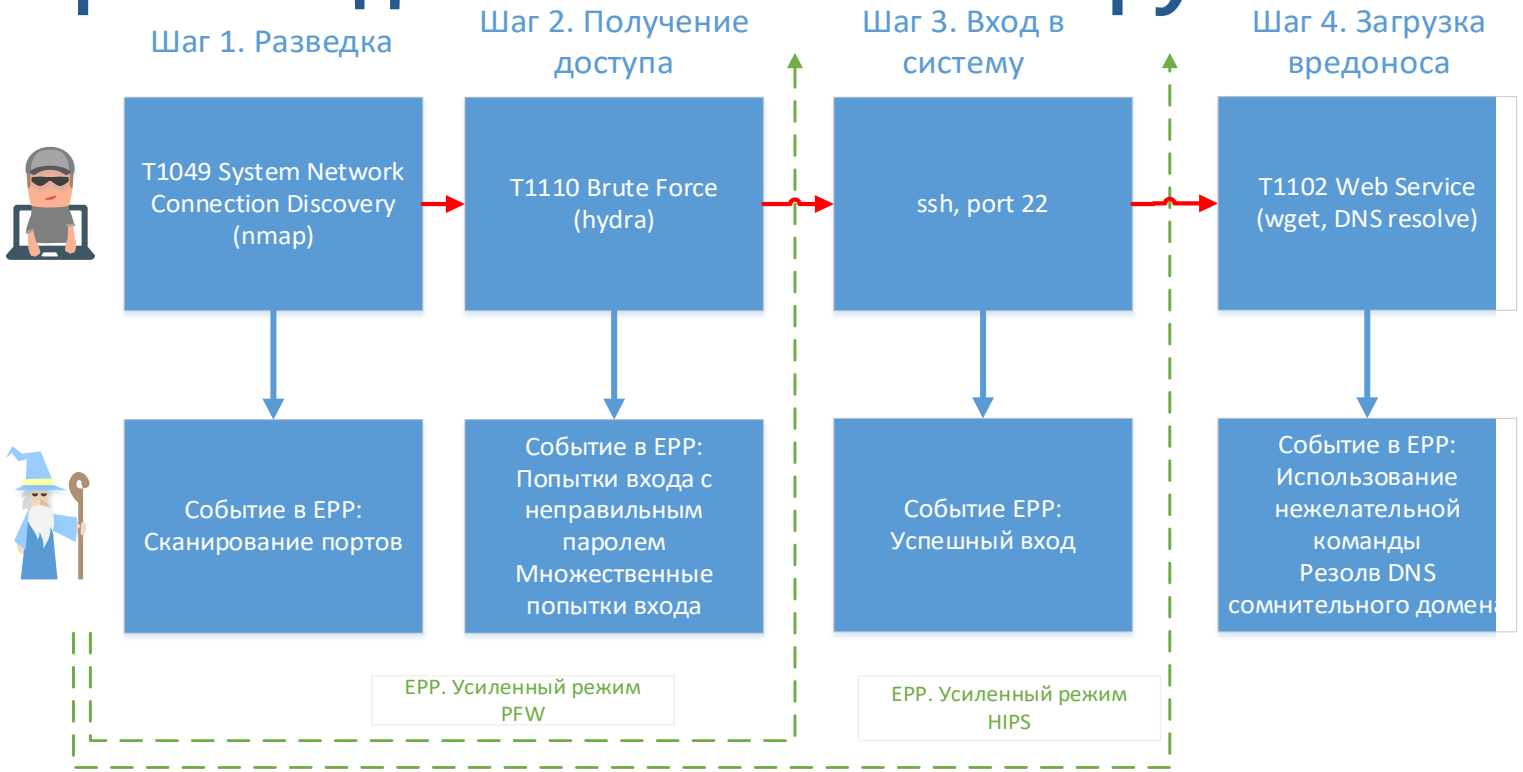
- Мониторинг и противодействие подозрительной активности на хосте
- Защита и предотвращение сетевых атак
- Защита от внедрения и выполнения вредоносных программ и кода
- Защита легитимных процессов



Пошаговый разбор. Как противодействовать хакеру



Пошаговый разбор.
Как противодействовать хакеру



ViPNet Zero Trust Architecture

Защищенное соединение

Построение шифрованного туннеля между узлами

ViPNet Client, ViPNet Coordinator HW/VA

Микропериметр

Контроль доступа пользователей к программам, файлам и документам, устройствам. Всё ПО и службы защищены от изменений. Комплексная защита конечных точек от атак и обнаружение и реагирование на вредоносные действия. Отслеживание работы антивируса

ViPNet EPP, ViPNet SafePoint

Микросегментация

Сегментация сети для обеспечения политик нулевого доверия. Разграничение доступа на прикладном уровне, безопасное подключение BYOD устройств и комплексная защита от сетевых угроз.

ViPNet Client, ViPNet Coordinator HW/VA, ViPNet xFirewall

Мониторинг и аналитика

Защита от внешних угроз, обнаружение и реагирование на неизвестные угрозы

ViPNet EPP, ViPNet IDS NS, ViPNet TIAS

Архитектра Zero Trust готова!

Выбор средств защиты

Анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение

- Выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей
- Анализ возможных уязвимостей значимого объекта и его программных, программно-аппаратных средств
- Определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации
- Оценку возможных последствий от реализации (возникновения) угроз безопасности информации

Выбор средств защиты

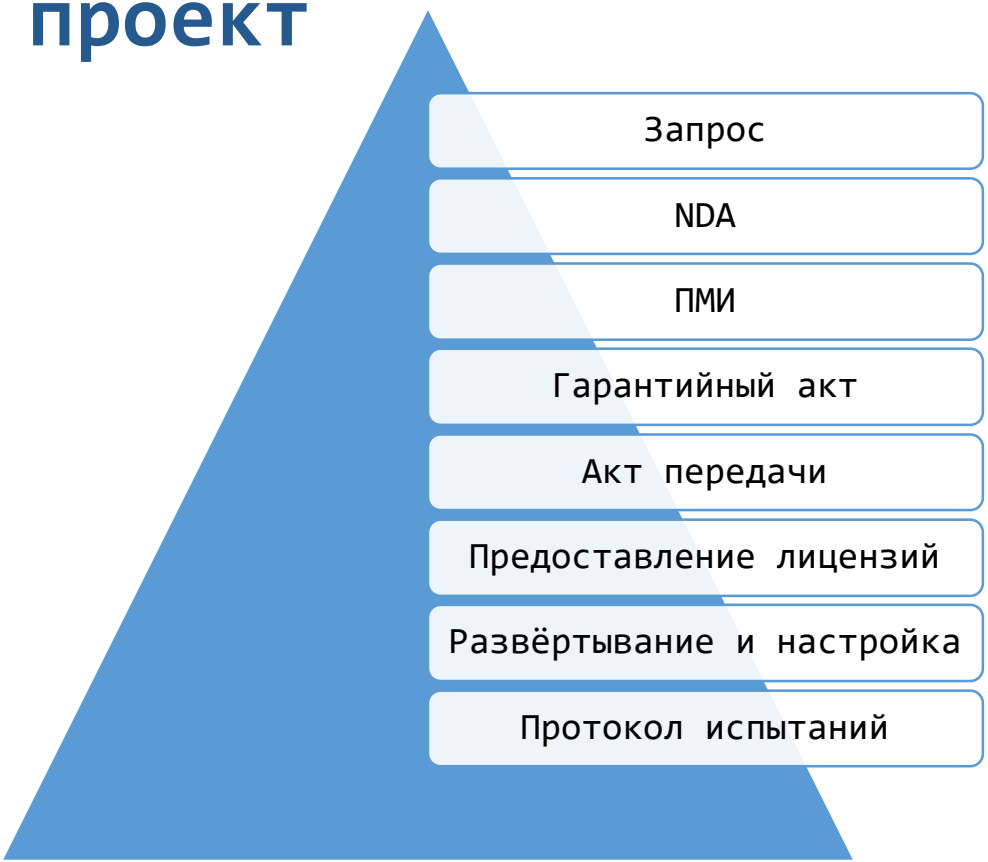
Проектирование подсистемы безопасности значимого объекта

- **определяются субъекты доступа** (пользователи, процессы и иные субъекты доступа) и объекты доступа;
- **определяются политики управления доступом** (дискреционная, мандатная, ролевая, комбинированная);
- **определяются и обосновываются организационные и технические меры**, подлежащие реализации в рамках подсистемы безопасности значимого объекта;
- **определяются виды и типы средств защиты информации**, обеспечивающие реализацию технических мер по обеспечению безопасности значимого объекта;
- **осуществляется выбор средств защиты информации** и (или) их разработка с учетом категории значимости значимого объекта, совместимости с программными и программно-аппаратными средствами, выполняемых функций безопасности и ограничений на эксплуатацию;
- **разрабатывается архитектура подсистемы безопасности** значимого объекта, включающая состав, места установки, взаимосвязи средств защиты информации;
- **определяются требования к параметрам настройки** программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, блокирование (нейтрализацию) угроз безопасности информации и устранение уязвимостей значимого объекта;
- **определяются меры по обеспечению безопасности** при взаимодействии значимого объекта с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями.

Макетирование

> В целях тестирования подсистемы безопасности значимого объекта в ходе проектирования может осуществляться ее макетирование или создание тестовой среды.

Пилотный проект



Спасибо за внимание!

Селифанов Валентин
Valentin.Selifanov@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363