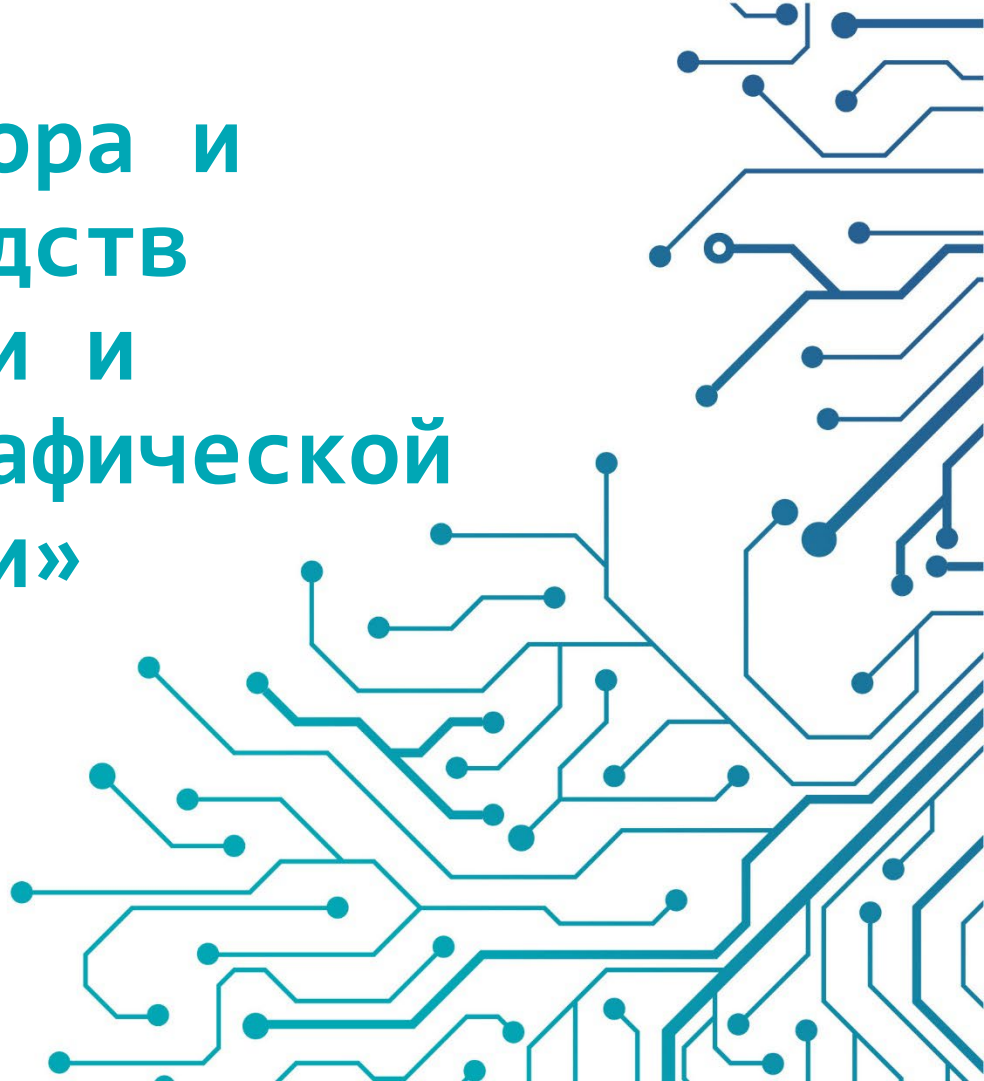
«Особенности выбора и эксплуатации средств защиты информации и средств криптографической защиты информации»

Селифанов Валентин
Заместитель руководителя обособленного подразделения



infotecs

От чего защищаемся?

От кого защищаемся?

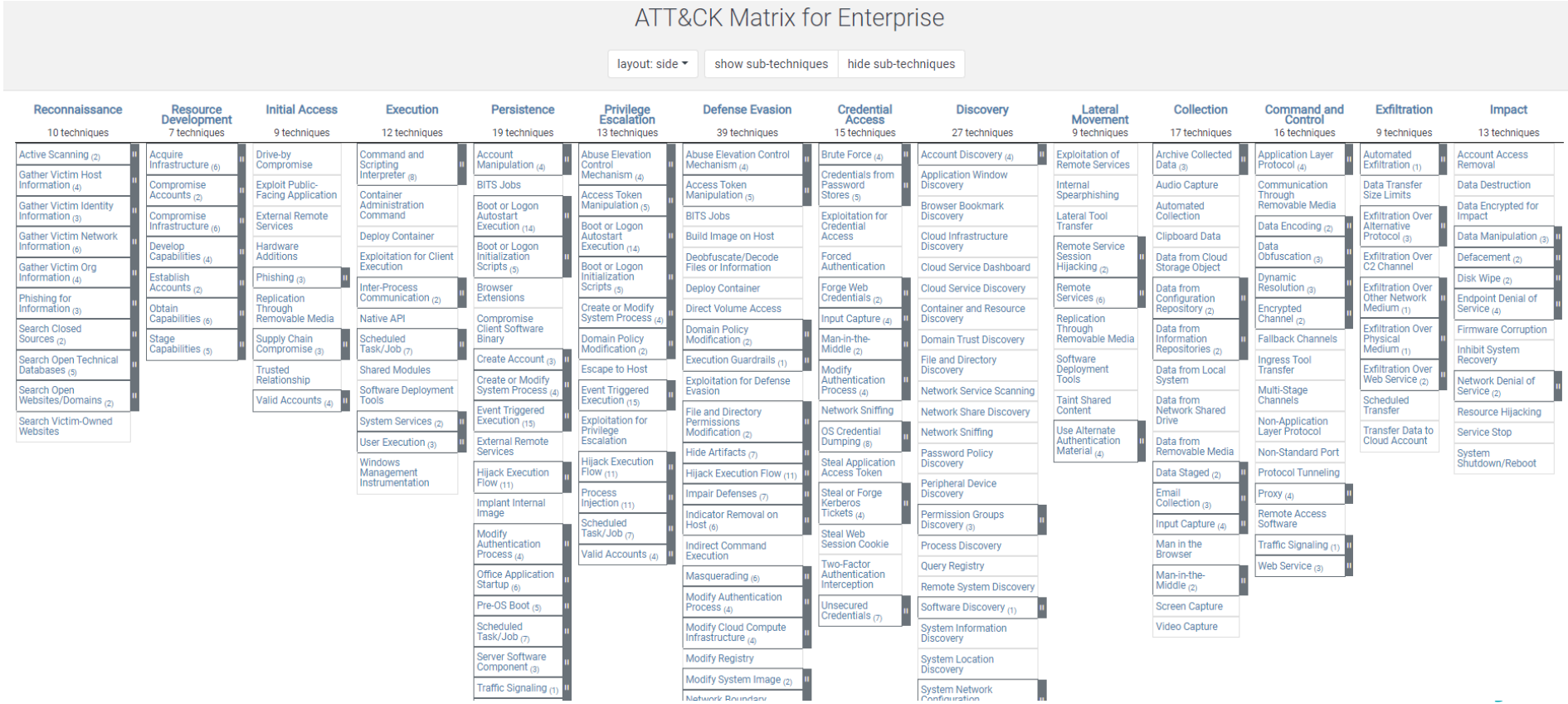
Инсайдеры

Иностранные вендоры, уходящие с рынка и отключающие свои продукты

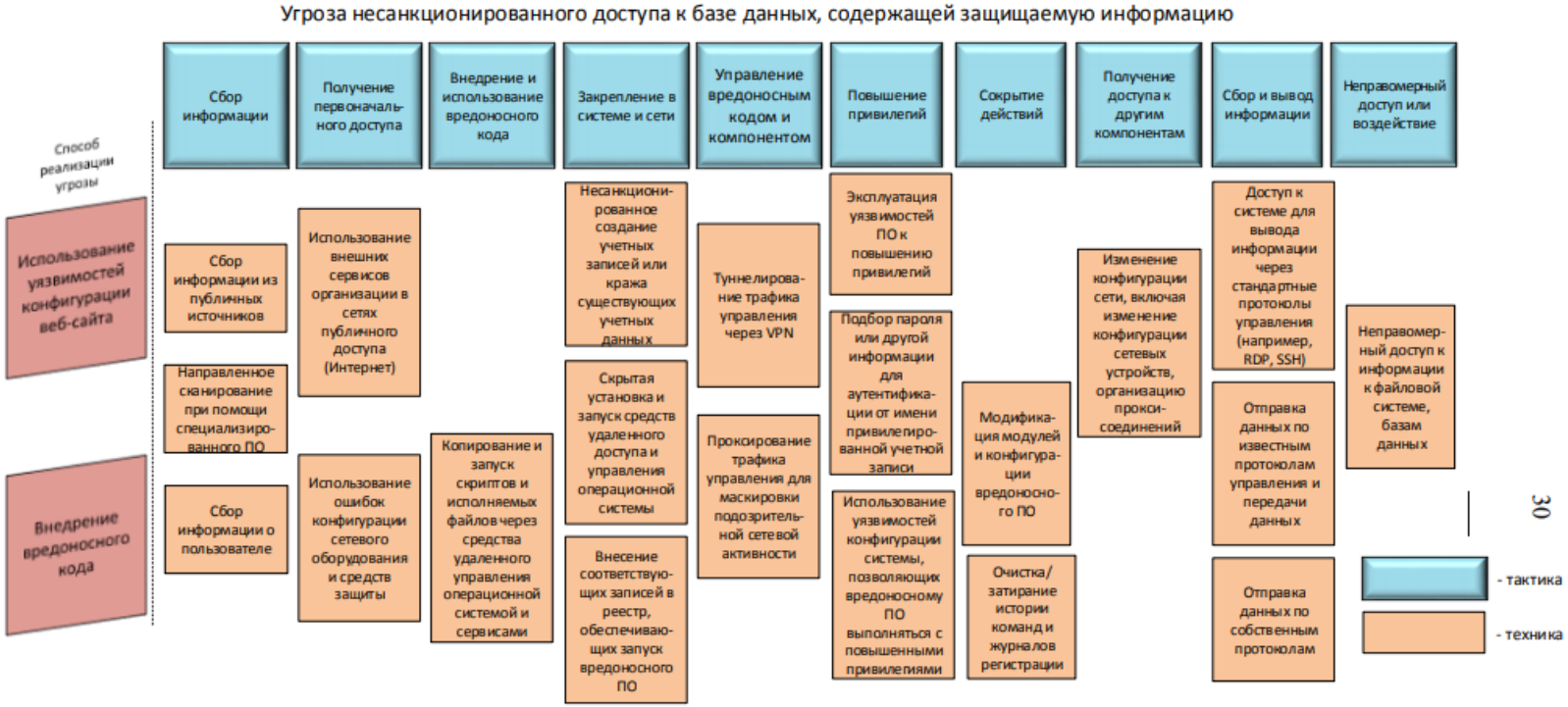
Хакеры

Техники — Тактики — Процедуры

infotecs



«Методика оценки угроз безопасности информации»



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

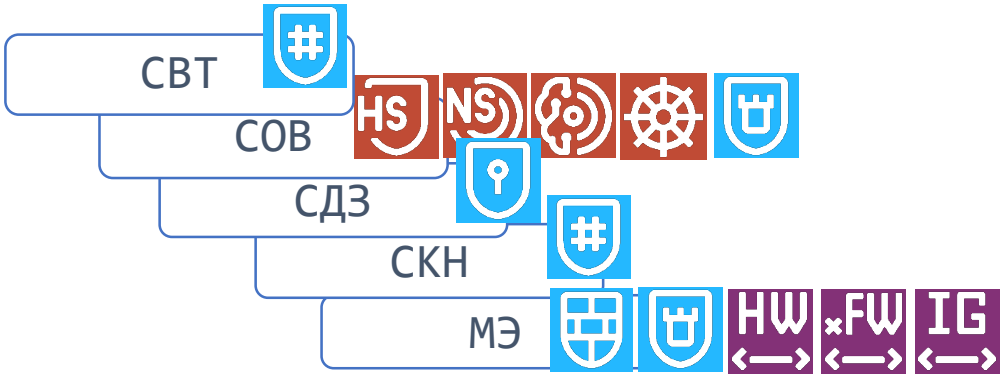
Выбор средств защиты

Проектирование подсистемы безопасности значимого объекта

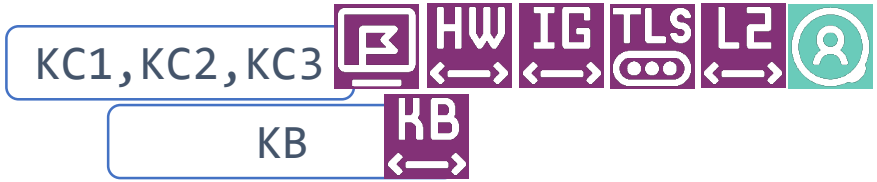
- **определяются субъекты доступа** (пользователи, процессы и иные субъекты доступа) и объекты доступа;
- **определяются политики управления доступом** (дискреционная, мандатная, ролевая, комбинированная);
- **определяются и обосновываются организационные и технические меры**, подлежащие реализации в 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.

Выбор средств защиты

ВИД СЗИ от НСД



СКЗИ



ЭКСПЛУАТАЦИЯ СИСТЕМЫ ЗИ

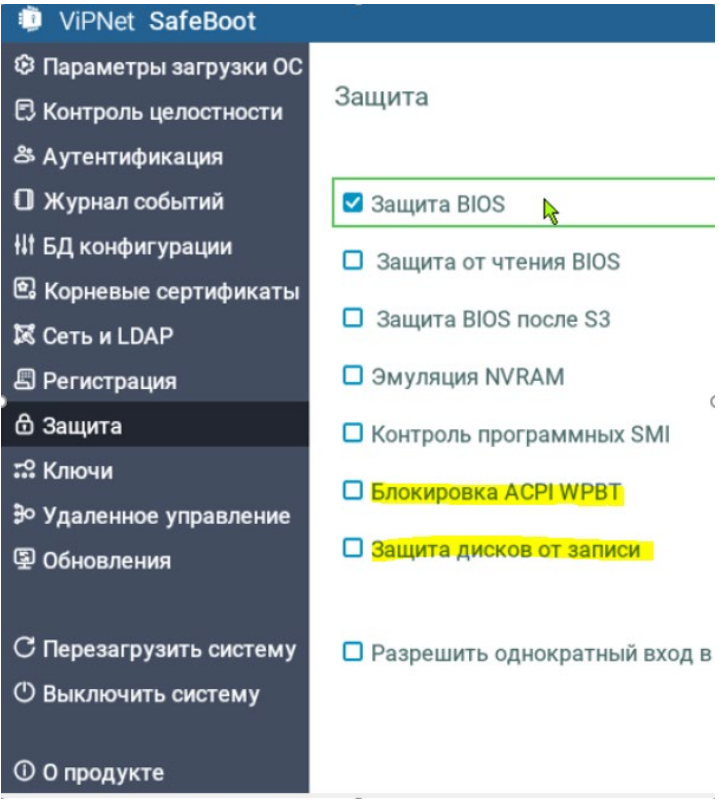
Техподдержка

Давайте попрактикуемся

Перечень угроз относящиеся к угрозам BIOS/UEFI

Угроза	Угроза
УБИ.004: Угроза аппаратного сброса пароля BIOS	УБИ.053: Угроза невозможности управления правами пользователей BIOS
УБИ.005: Угроза внедрения вредоносного кода в BIOS	УБИ.072: Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
УБИ.008: Угроза восстановления аутентификационной информации	УБИ.087: Угроза несанкционированного использования привилегированных функций BIOS
УБИ.006: Угроза внедрения кода или данных	УБИ.090: Угроза несанкционированного создания учётной записи пользователя
УБИ.009: Угроза восстановления предыдущей уязвимой версии BIOS	УБИ.108: Угроза ошибки обновления гипервизора
УБИ.013: Угроза деструктивного использования декларированного функционала BIOS	**УБИ.121: Угроза повреждения системного реестра**
УБИ.018: Угроза загрузки нештатной операционной системы	УБИ.123: Угроза подбора пароля BIOS
УБИ.023: Угроза изменения компонентов системы	УБИ.124: Угроза подделки записей журнала регистрации событий
УБИ.024: Угроза изменения режимов работы аппаратных элементов компьютера	УБИ.129: Угроза подмены резервной копии программного обеспечения BIOS
УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию	УБИ.144: Угроза программного сброса пароля BIOS
УБИ.032: Угроза использования поддельных цифровых подписей BIOS	**УБИ.145: Угроза пропуска проверки целостности программного обеспечения**
УБИ.035: Угроза использования слабых криптографических алгоритмов BIOS	УБИ.150: Угроза сбоя процесса обновления BIOS
УБИ.039: Угроза исчерпания запаса ключей, необходимых для обновления BIOS	УБИ.152: Угроза удаления аутентификационной информации
УБИ.045: Угроза нарушения изоляции среды исполнения BIOS	УБИ.154: Угроза установки уязвимых версий обновления программного обеспечения BIOS
	УБИ.179: Угроза несанкционированной модификации защищаемой информации

ViPNet SafeBoot



Защита от malware в UEFI BIOS

Активация защиты на платформах AMD

Поддержка токена Rutoken S

Поддержка работы со считывателями смарт-карт – ACR38, JCR721, ASEDrive IIIe

Поддержка SSO для входа в операционную систему и ViPNet SafePoint v.1.2

Поддержка сенсорных экранов, реализация сенсорной клавиатуры под UEFI

Базовая поддержка ARM-архитектуры

ViPNet SafeBoot

Организация доверенной загрузки

Контроль целостности

Разграничение доступа

- UEFI BIOS
- MBR
- Таблицы ACPI, SMBIOS, карты распределения памяти
- Файлов
- CMOS
- Двухфакторная аутентификация
- Авторизация в AD/LDAP

Перечень актуальных угроз

УБИ.015: Угроза доступа к защищаемым файлам с использованием обходного пути

УБИ.031: Угроза использования механизмов авторизации для повышения привилегий

УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией

УБИ.088: Угроза несанкционированного копирования защищаемой информации

УБИ.091: Угроза несанкционированного удаления защищаемой информации

УБИ.122: Угроза повышения привилегий

УБИ.143: Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации

УБИ.161: Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями

УБИ.170: Угроза неправомерного шифрования информации

ViPNet SafePoint

- Контроль входа пользователей в систему
- Реализация замкнутой программной среды, разграничивает доступ к файлам
- Защита от олицетворения прав пользователя, тем самым не позволяет получать доступ к ПО и файлам от лица других пользователей системы
- Контроль и разграничение права на отключение и подключение к системе различных устройств
- Контроль целостности заданных файлов и объектов реестра ОС с возможностью автоматического восстановления их эталонного состояния в случае модификации

Перечень угроз

УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией

УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети

УБИ.098: Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб

УБИ.167: Угроза заражения компьютера при посещении неблагонадёжных сайтов

УБИ.175: Угроза «фишинга»

УБИ.178: Угроза несанкционированного использования системных и сетевых утилит

ViPNet EndPoint Protection

Обнаружение и предотвращение атак

Используем:

- Эвристический анализ
- Сигнатурный анализ

Следим за:

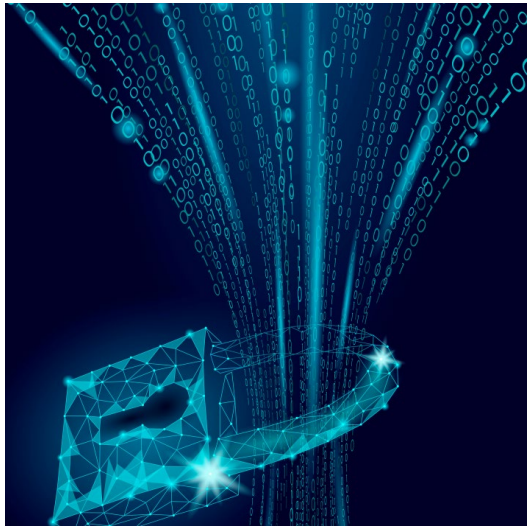
- Системными журналами Windows
- Журналами и логами приложений
- Изменениями в файловой системе и реестре
- Сетевым трафиком

Блокируем:

- Подозрительный сетевой трафик
- Атакующие хосты

Межсетевое экранирование

- Фильтрация трафика Ipv4 и Ipv6
- Работа сетевых фильтров по расписанию
- Наличие преднастроенных фильтров
- Создание фильтров для определенных групп хостов
- Создание правил фильтрации из журнала трафика

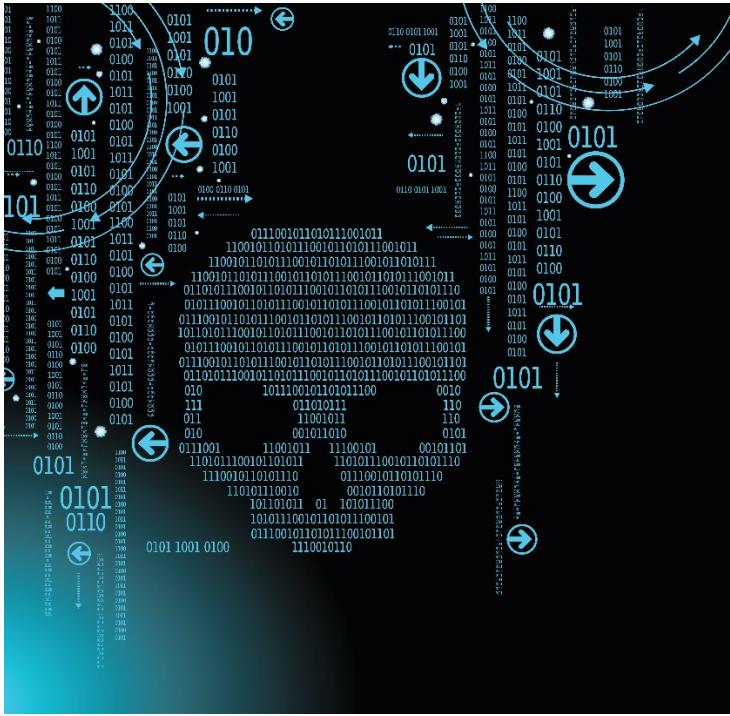


Контроль приложений

- Контроль запуска программ с использованием Черных и Белых списков программного обеспечения
- Анализ командной строки
- Защита файлов
- Защита реестра
- Контроль запуска программ, DLL-модулей, драйверов
- Контроль сетевой активности приложений

Эвристический Antimalware движок

- Возможность сканирования исполняемых файлов и библиотек с целью выявления зловреда
- Эвристический Antimalware использует собственную модель построенную с помощью машинного обучения
- Модель постоянно обновляется в рамках подписки на БРП



Модуль поведенческого анализа

Используем модель нормальной активности защищаемого узла, построенной с помощью машинного обучения.

Выявляем различного рода аномалии, например:

- Аномальный вход в систему
- Аномалия в создании процесса
- Аномалия в создании задачи планировщику
- Аномальные запуски системных утилит, таких как powershell, rundll32, regsrv32 и т.д.

Обнаружение и предотвращение бесфайловых атак

- Расширение возможностей модуля обнаружения и предотвращения вторжений
- Отслеживаем техники Keylogging и Process injection
  - Credential API Hooking (T1056.004)
  - Process Hollowing (T1055.012)
  - Process Doppelganging (T1055.013)
  - Dynamic-link library injection (T1055.001)
  - Portable Executable Injection (T1055.002)

Перечень угроз

УБИ.003: Угроза использования слабостей криптографических алгоритмов и уязвимостей в программном обеспечении их реализации;

УБИ.036: Угроза использования слабостей протоколов сетевого/локального обмена данным;

УБИ.098: Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб

УБИ.082: Угроза несанкционированного доступа к сегментам вычислительного поля

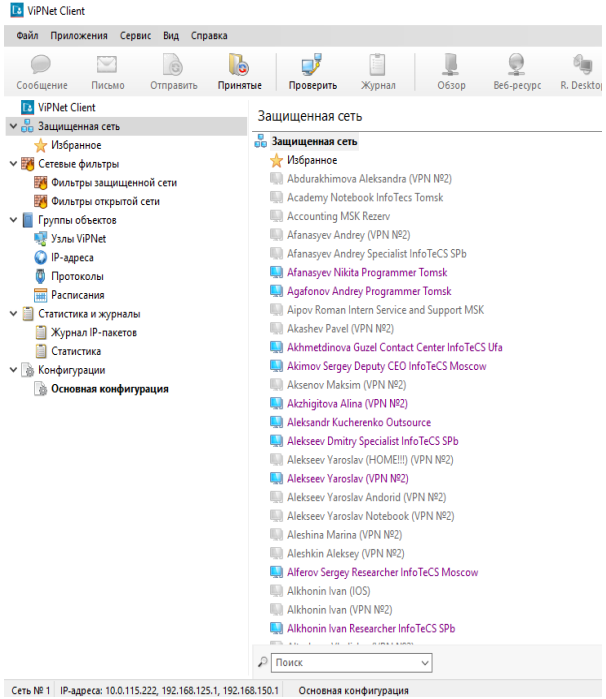
УБИ.083: Угроза несанкционированного доступа к системе по беспроводным каналам

УБИ.104: Угроза определения топологии вычислительной сети

УБИ.116: Угроза перехвата данных, передаваемых по вычислительной сети

УБИ.128: Угроза подмены доверенного пользователя

ViPNet Client



- VPN-соединение с использованием технологии ViPNet по IP адресу/DNS имени или внутреннему идентификатору узла сети ViPNet
- Двухфакторная аутентификация
- Прозрачен для приложений пользователя и сервисов ОС
- Совместим с ПО ViPNet «Деловая почта»
- Поддержку Windows, Linux, MacOS, Android, iOS, Aurora (Sailfish)

ViPNet Coordinator HW

- Криптографическая защита каналов связи
- Межсетевое экранирование до 4 уровня модели OSI
- Сегментирование сети
- Сетевые и сервисные функции
- Доверенная платформа

Сертификаты:

- ФСБ России - СКЗИ класса – КС1,КС3, МЭ – 4 класса
- ФСТЭК России – МЭ типа «А», «Б» - 4 класса, ТДБ - 4 уровень

Перечень угроз

УБИ.073: Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети

УБИ.082: Угроза несанкционированного доступа к сегментам вычислительного поля

УБИ.083: Угроза несанкционированного доступа к системе по беспроводным каналам

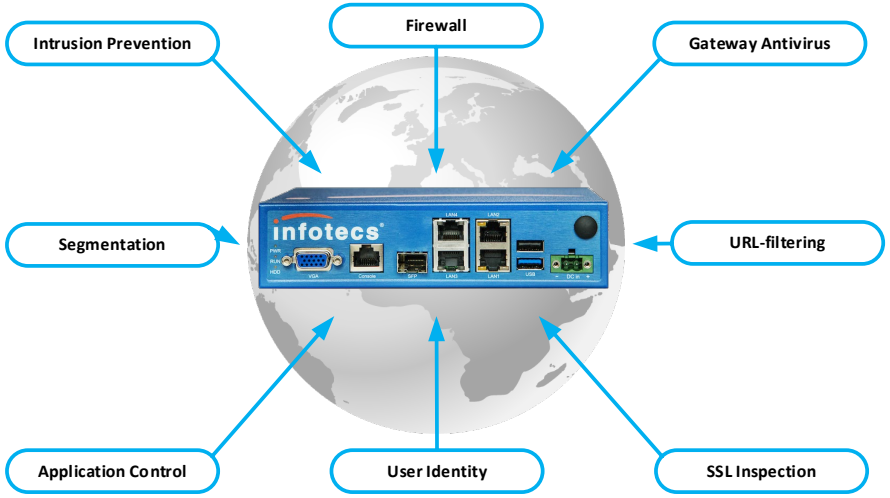
УБИ.085: Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации

УБИ.167: Угроза заражения компьютера при посещении неблагонадёжных сайтов

УБИ.172: Угроза распространения «почтовых червей»

УБИ.178: Угроза несанкционированного использования системных и сетевых утилит

ViPNet xFirewall



- Межсетевое экранирование до 7 уровня модели OSI
- Сегментирование сети, сетевые и сервисные функции
- Система предотвращения атак IPS
- Система контроля приложений
- SSL- инспекция
- URL- фильтрация

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