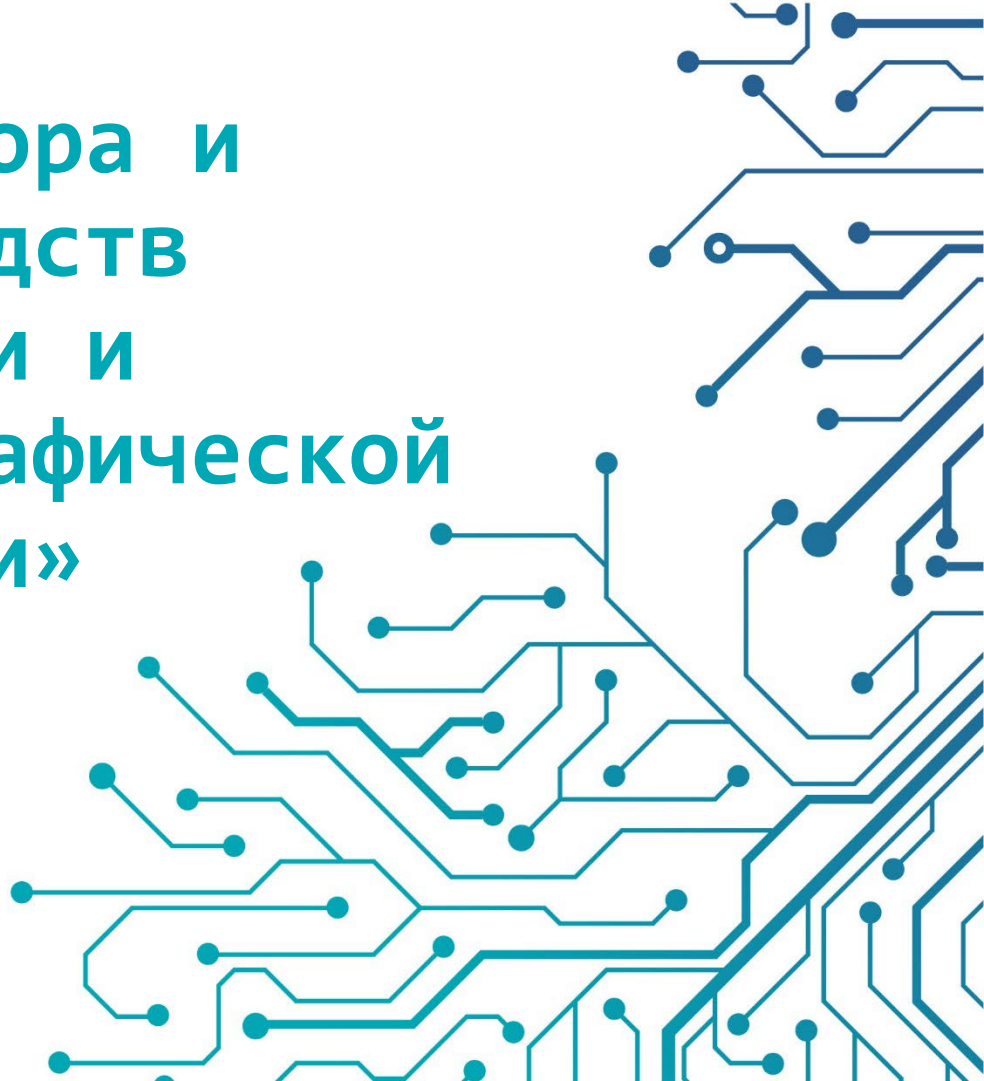
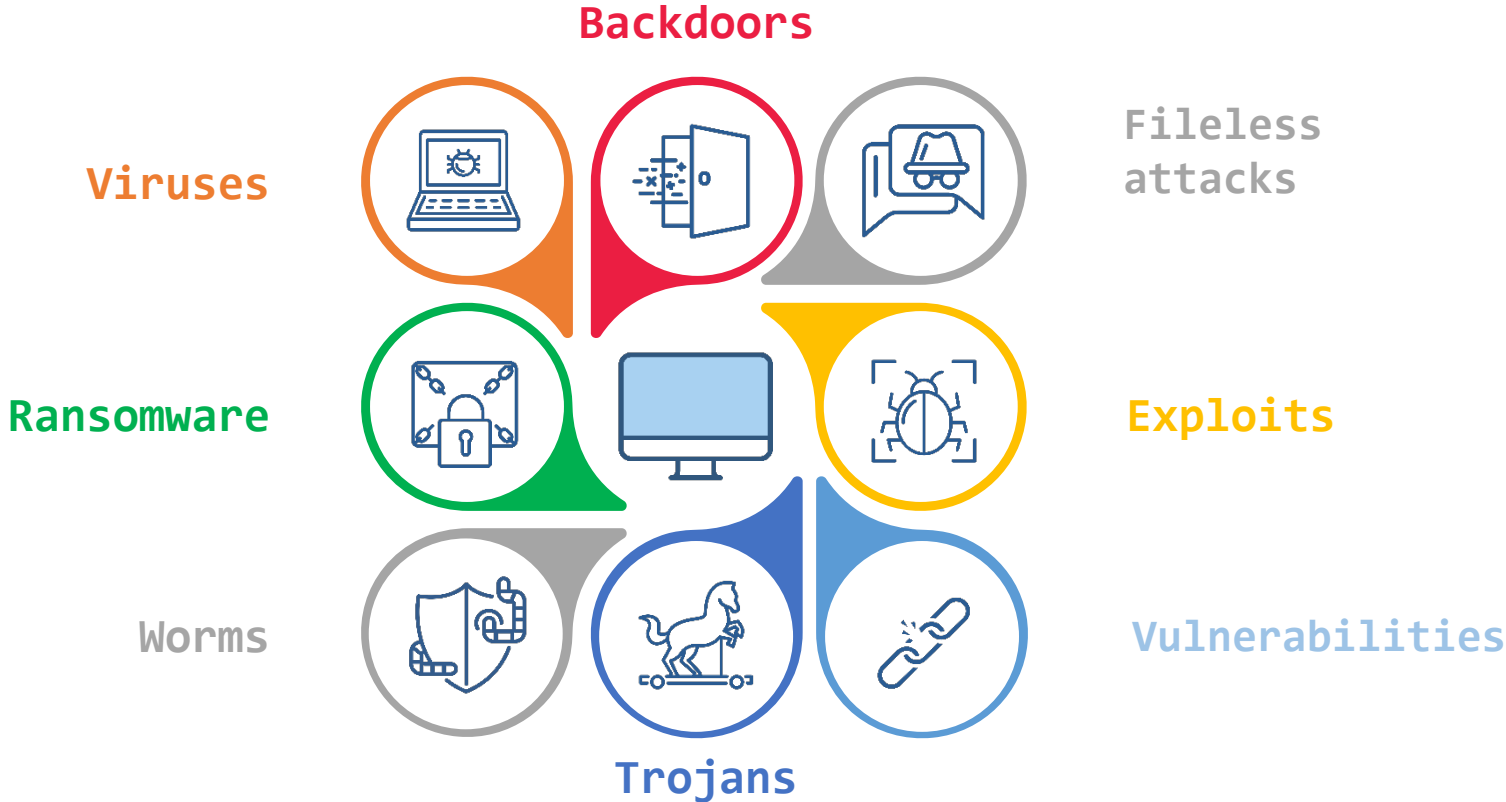


«Особенности выбора и эксплуатации средств защиты информации и средств криптографической защиты информации»

Селифанов Валентин
Заместитель руководителя
обособленного подразделения



От чего защищаемся?



От кого защищаемся?



Инсайдеры



Иностранные вендоры,
уходящие с рынка и
отключающие свои продукты



Хакеры

Техники — Тактики — Процедуры

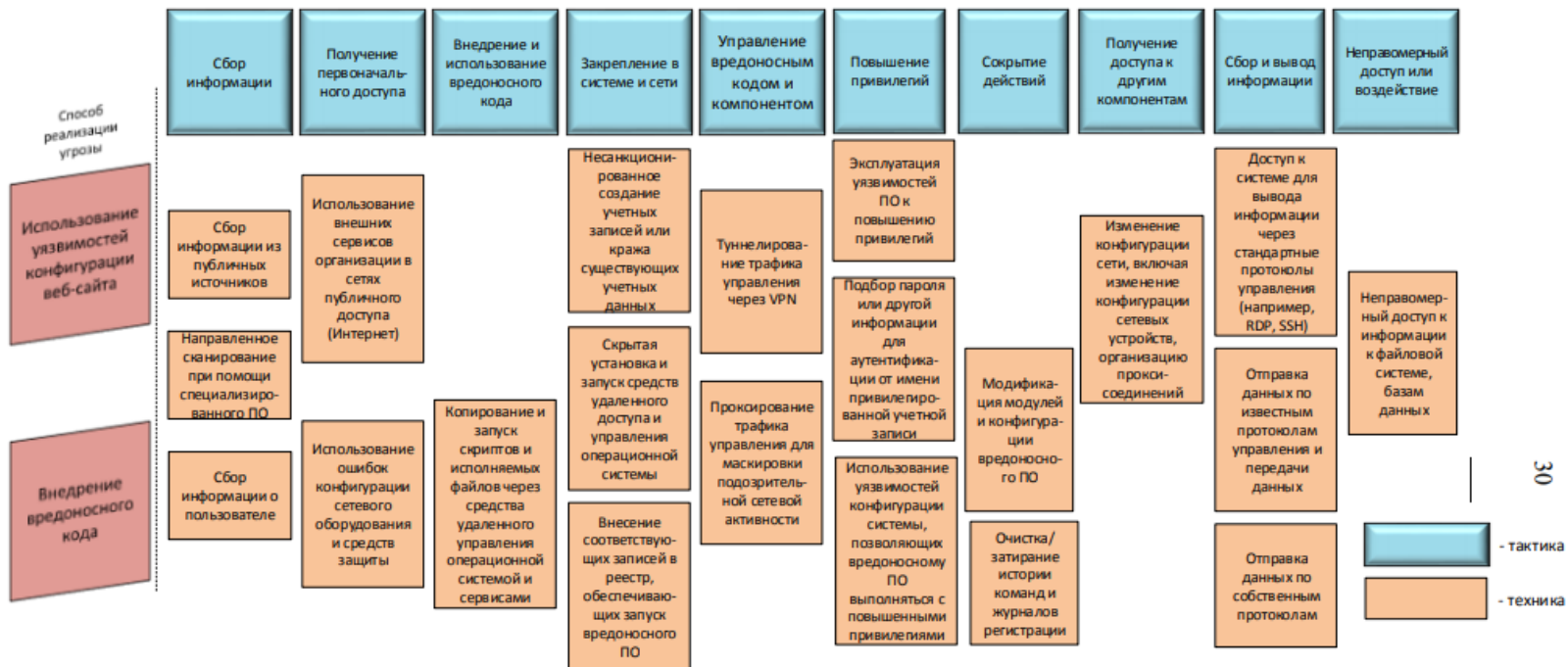
ATT&CK Matrix for Enterprise

layout: side ▾ show sub-techniques hide sub-techniques

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (9)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (5)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Access Token Manipulation (5)	Access Token Manipulation (5)	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Build Image on Host	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Create or Modify System Process (4)	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (7)	Create Account (3)	Domain Policy Modification (2)	Domain Policy Modification (2)	Man-in-the-Middle (2)	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories (2)	Fallback Channels	Exfiltration Over Web Service (2)	Firmware Corruption
Search Open Technical Databases (5)	Trusted Relationship	Valid Accounts (4)	Shared Modules	Create or Modify System Process (4)	Escape to Host	Escape to Host	Modify Authentication Process (4)	Domain Trust Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Open Websites/Domains (2)	User Execution (3)		Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Network Sniffing	File and Directory Permissions Modification (2)	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Exfiltration Over Web Service (2)	Network Denial of Service (2)
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (11)	Hijack Execution Flow (11)	OS Credential Dumping (8)	Network Share Discovery		Data from Network Shared Drive	Non-Application Layer Protocol	Scheduled Transfer	Resource Hijacking
			User Execution (3)	Hijack Execution Flow (11)	Impair Defenses (7)	Impair Defenses (7)	Steal Application Access Token	Network Sniffing		Data from Removable Media	Non-Standard Port	Transfer Data to Cloud Account	Service Stop
			Windows Management Instrumentation	Hijack Execution Flow (11)	Indicator Removal on Host (6)	Indicator Removal on Host (6)	Steal Web Session Cookie	Password Policy Discovery		Data Staged (2)	Protocol Tunneling		System Shutdown/Reboot
				Implant Internal Image	Indirect Command Execution	Indirect Command Execution	Steal or Forge Kerberos Tickets (4)	Peripheral Device Discovery		Email Collection (3)	Proxy (4)		
				Modify Authentication Process (4)	Process Injection (11)	Process Injection (11)	Permission Groups Discovery (3)	Process Discovery		Input Capture (4)	Remote Access Software		
				Office Application Startup (6)	Scheduled Task/Job (7)	Scheduled Task/Job (7)	Query Registry	Remote System Discovery		Man in the Browser	Traffic Signaling (1)		
				Pre-OS Boot (5)	Valid Accounts (4)	Valid Accounts (4)	Remote System Discovery	Software Discovery (1)		Man-in-the-Middle (2)	Web Service (3)		
				Scheduled Task/Job (7)			System Information Discovery	System Information Discovery		Screen Capture			
				Server Software Component (3)			System Location Discovery	System Location Discovery		Video Capture			
				Traffic Signaling (1)			System Network Configuration	System Network Configuration					
							Network Boundary						

«Методика оценки угроз безопасности информации»

Угроза несанкционированного доступа к базе данных, содержащей защищаемую информацию



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

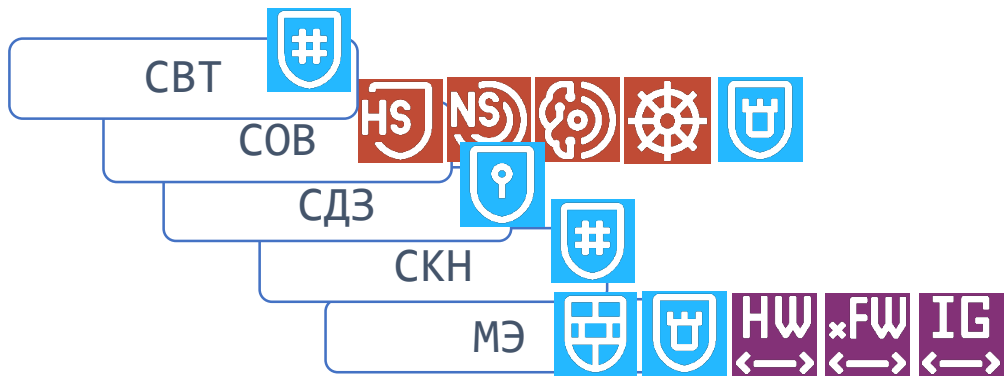
Выбор средств защиты

Проектирование подсистемы безопасности значимого объекта

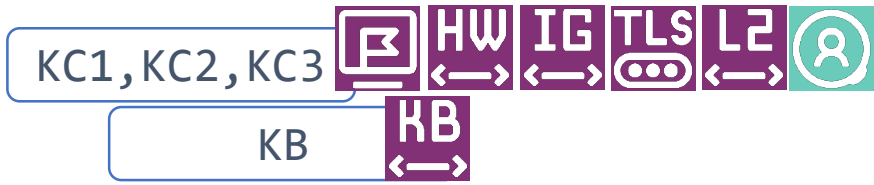
- **определяются субъекты доступа** (пользователи, процессы и иные субъекты доступа) и объекты доступа;
- **определяются политики управления доступом** (дискреционная, мандатная, ролевая, комбинированная);
- **определяются и обосновываются организационные и технические меры**, подлежащие реализации в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

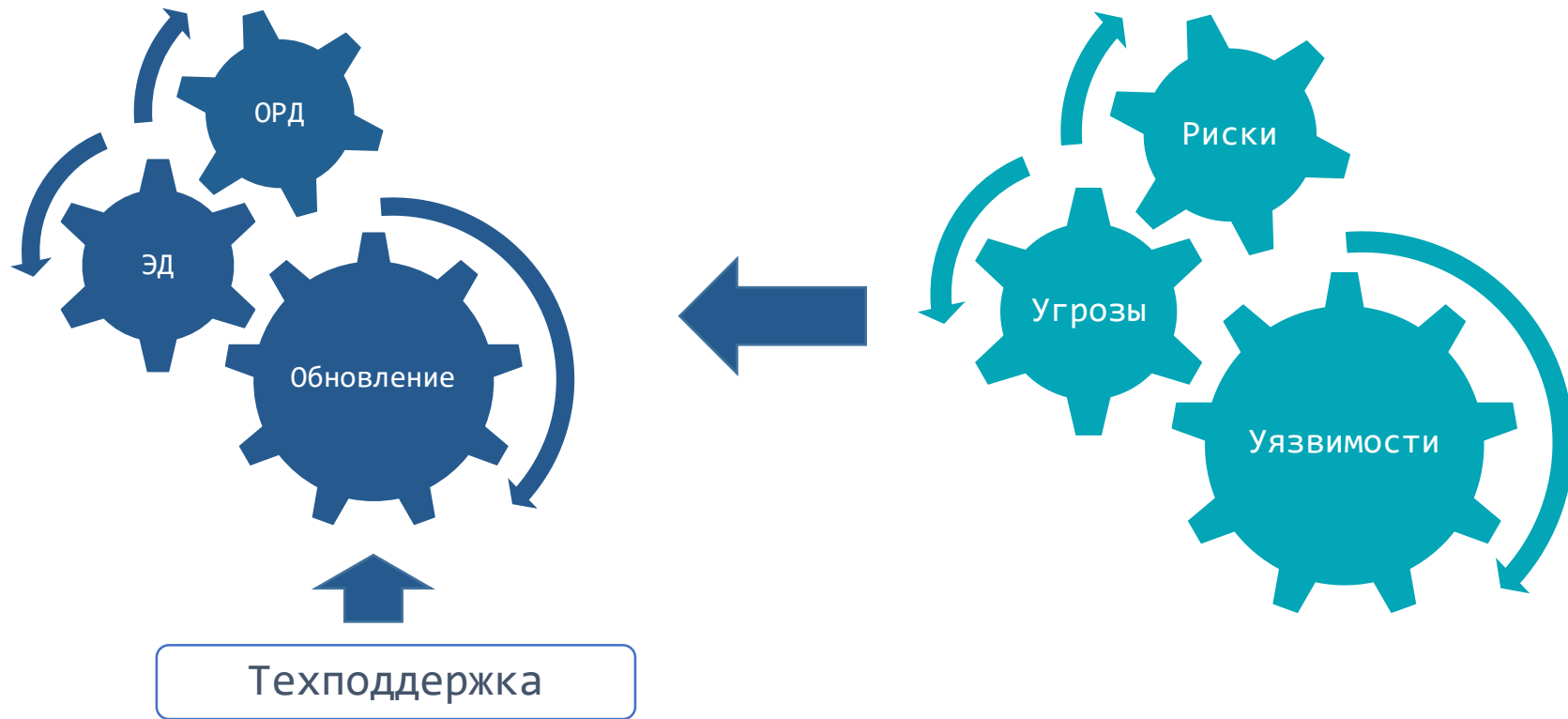
ВИД СЗИ от НСД



СКЗИ



ЭКСПЛУАТАЦИЯ СИСТЕМЫ ЗИ





**Давайте
попрактикуемся**

Перечень угроз относящиеся к угрозам BIOS/UEFI

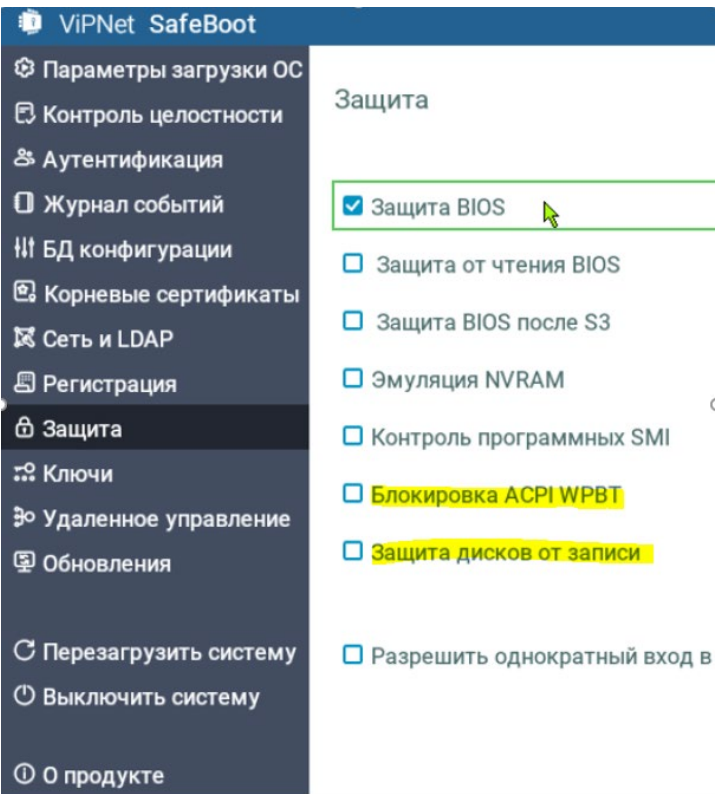
Угроза

- УБИ.004: Угроза аппаратного сброса пароля BIOS
- УБИ.005: Угроза внедрения вредоносного кода в BIOS
- УБИ.008: Угроза восстановления аутентификационной информации
- УБИ.006: Угроза внедрения кода или данных
- УБИ.009: Угроза восстановления предыдущей уязвимой версии BIOS
- УБИ.013: Угроза деструктивного использования декларированного функционала BIOS
- УБИ.018: Угроза загрузки нештатной операционной системы**
- УБИ.023: Угроза изменения компонентов системы
- УБИ.024: Угроза изменения режимов работы аппаратных элементов компьютера**
- УБИ.030: Угроза использования информации идентификации/аутентификации, заданной по умолчанию
- УБИ.032: Угроза использования поддельных цифровых подписей BIOS
- УБИ.035: Угроза использования слабых криптографических алгоритмов BIOS
- УБИ.039: Угроза исчерпания запаса ключей, необходимых для обновления BIOS
- УБИ.045: Угроза нарушения изоляции среды исполнения BIOS

Угроза

- УБИ.053: Угроза невозможности управления правами пользователей BIOS
- УБИ.072: Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
- УБИ.087: Угроза несанкционированного использования привилегированных функций BIOS
- УБИ.090: Угроза несанкционированного создания учётной записи пользователя
- УБИ.108: Угроза ошибки обновления гипервизора
- УБИ.121: Угроза повреждения системного реестра**
- УБИ.123: Угроза подбора пароля BIOS
- УБИ.124: Угроза подделки записей журнала регистрации событий
- УБИ.129: Угроза подмены резервной копии программного обеспечения BIOS
- УБИ.144: Угроза программного сброса пароля BIOS
- УБИ.145: Угроза пропуска проверки целостности программного обеспечения**
- УБИ.150: Угроза сбоя процесса обновления BIOS
- УБИ.152: Угроза удаления аутентификационной информации
- 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

Контроль приложений



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

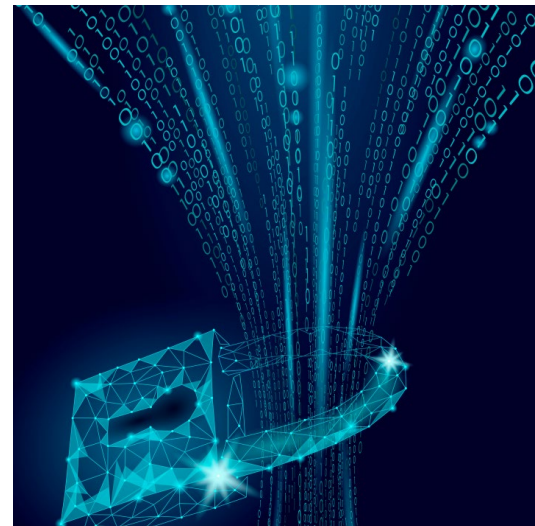
Блокируем:

- Подозрительный сетевой трафик
- Атакующие хосты



Межсетевое экранирование

- Фильтрация трафика Ipv4 и Ipv6
- Работа сетевых фильтров по расписанию
- Наличие предустановленных 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.

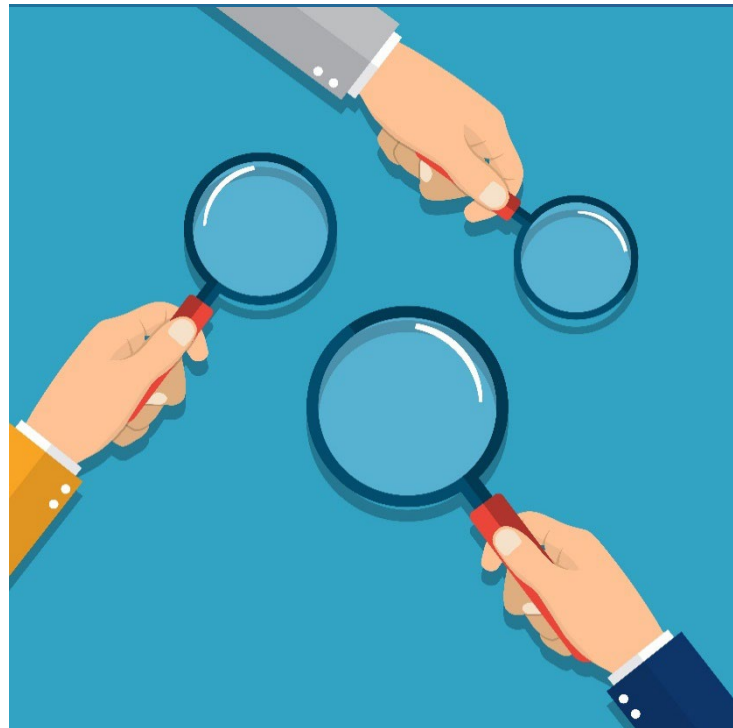
Выявляем различного рода аномалии, например:

- 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

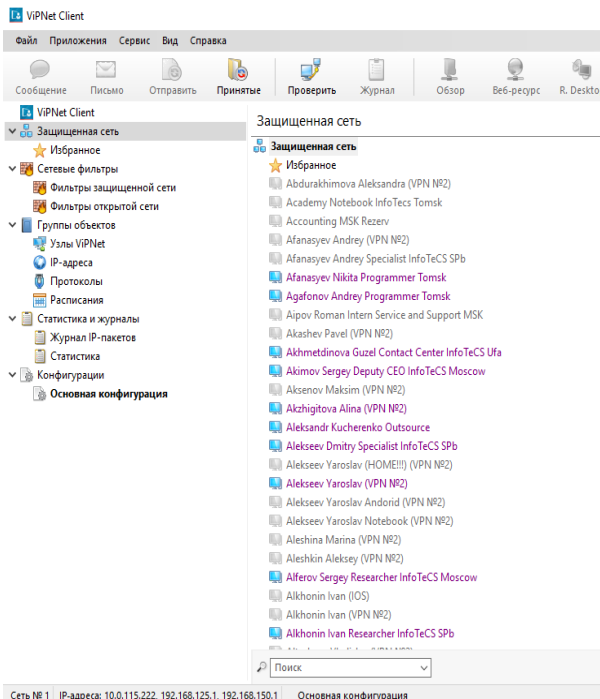
УБИ.083: Угроза несанкционированного доступа к системе по беспроводным каналам

УБИ.104: Угроза определения топологии вычислительной сети

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

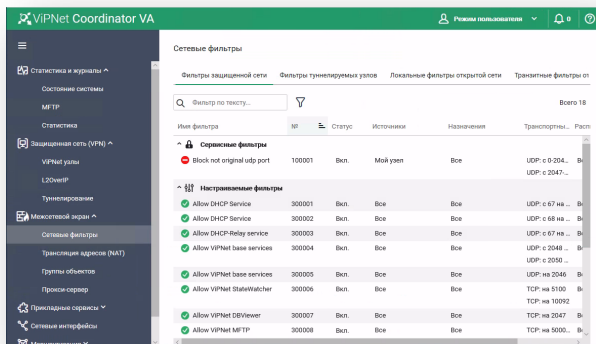
УБИ.128: Угроза подмены доверенного пользователя

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

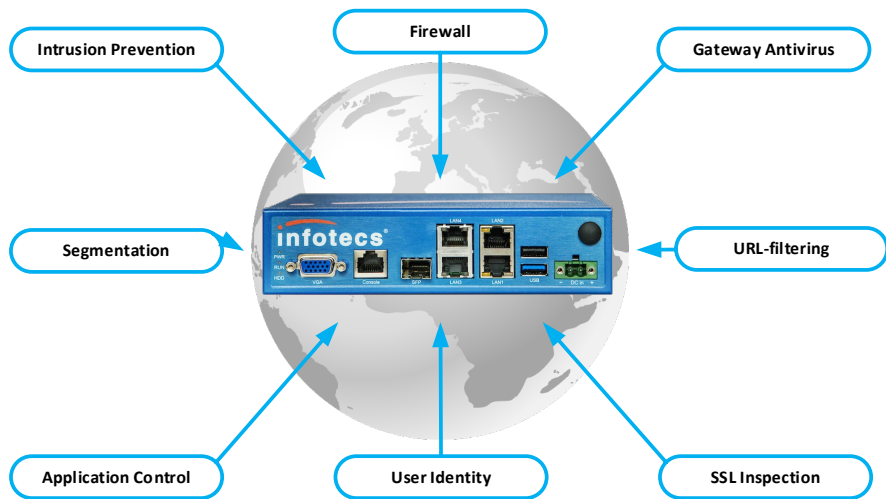
УБИ.085: Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации

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

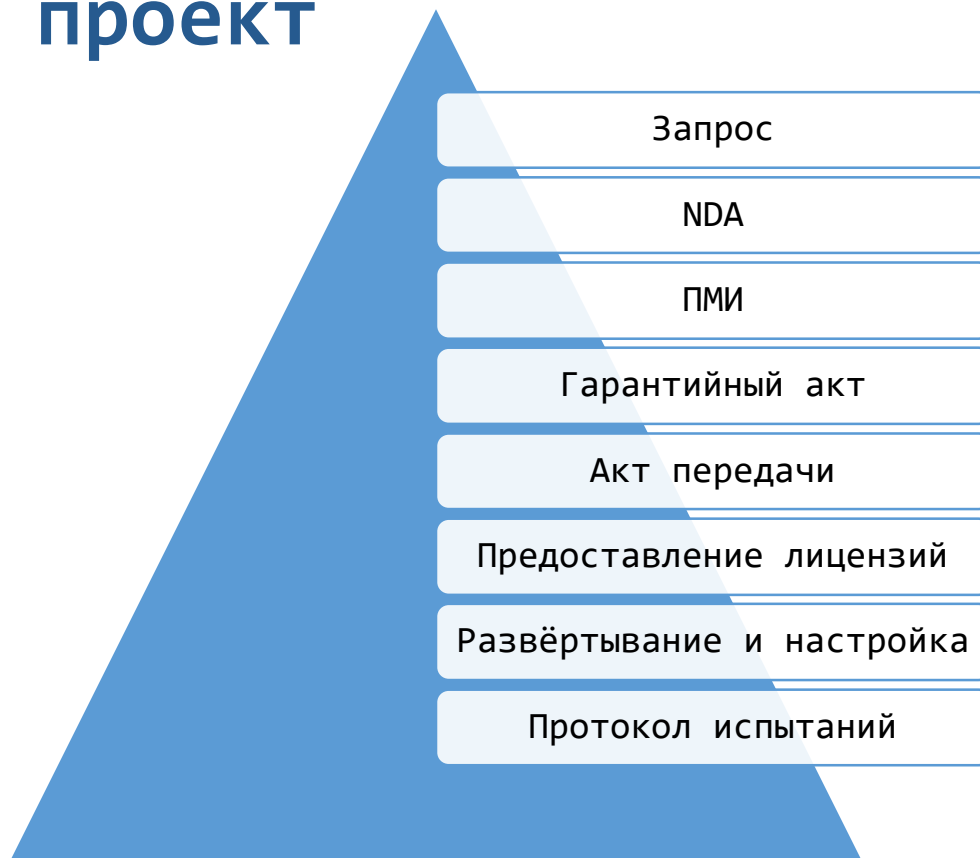


- Межсетевое экранирование до 7 уровня модели OSI
- Сегментирование сети, сетевые и сервисные функции
- Система предотвращения атак IPS
- Система контроля приложений
- SSL- инспекция
- URL- фильтрация

Макетирование

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

Пилотный проект





infotecs

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