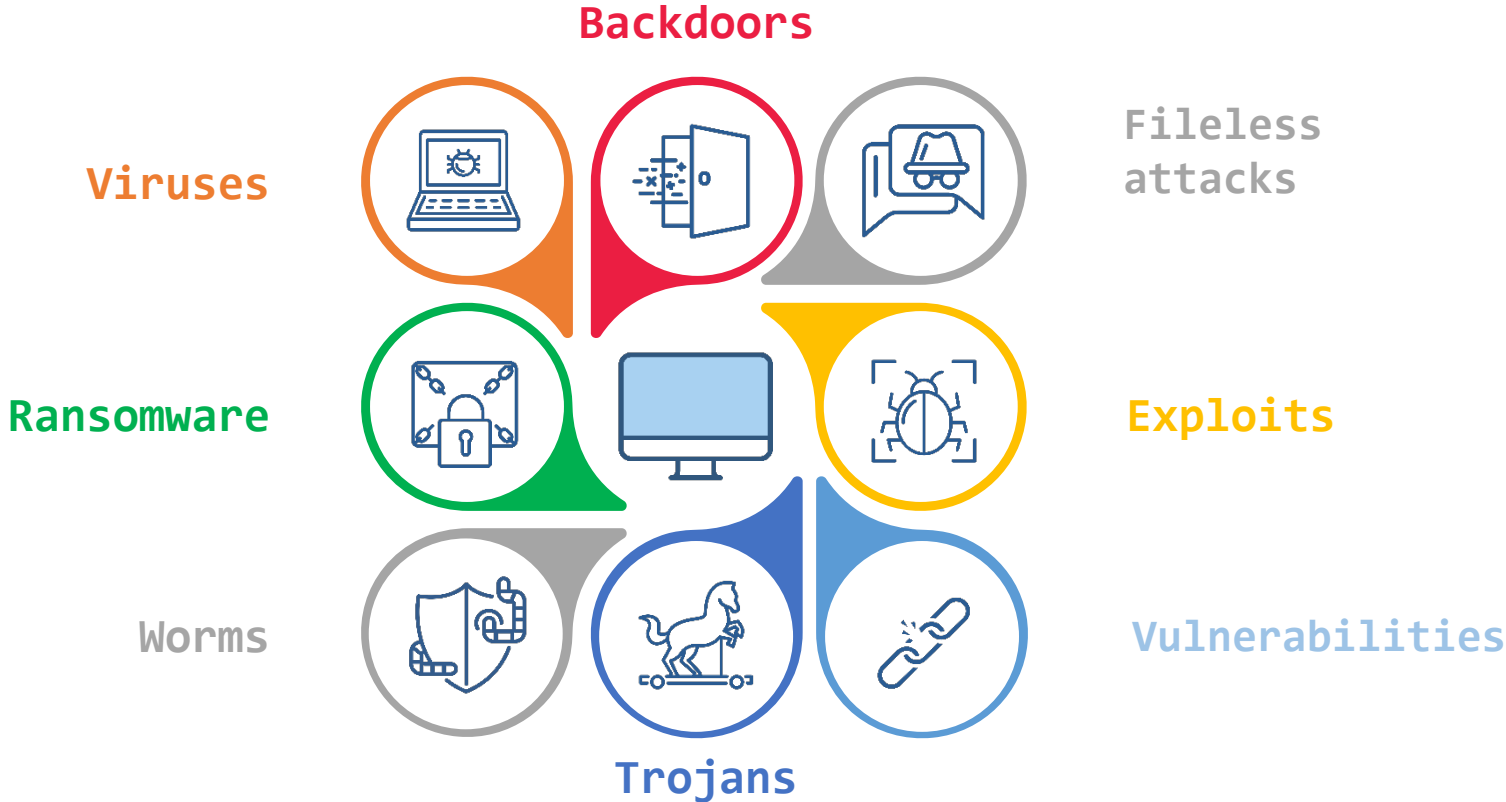


# «Особенности выбора и эксплуатации средств защиты информации и средств криптографической защиты информации»

Селифанов Валентин  
Заместитель руководителя  
обособленного подразделения



# От чего защищаемся?



# От кого защищаемся?



Инсайдеры



Иностранные вендоры,  
уходящие с рынка и  
отключающие свои продукты



Хакеры

# Как защищаемся?



# Техники — Тактики — Процедуры

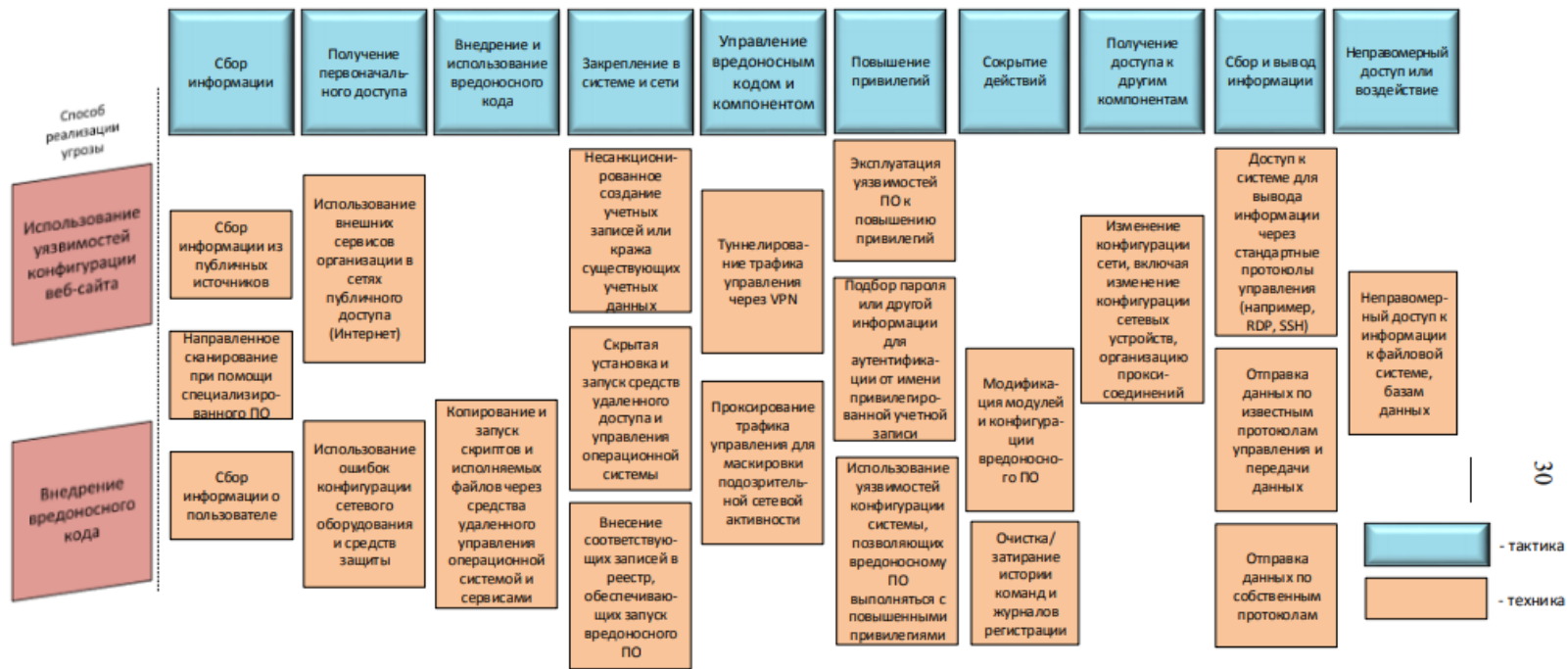
## ATT&CK Matrix for Enterprise

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)	BITS Jobs	BITS Jobs	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	Deobfuscate/Decode Files or Information	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	Deploy Container	Deploy Container	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	Direct Volume Access	Direct Volume Access	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)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Trusted Relationship	Valid Accounts (4)	Shared Modules	Create or Modify System Process (4)	Execution Guardrails (1)	Execution Guardrails (1)	Modify Authentication Process (4)	File and Directory Discovery	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Firmware Corruption	Inhibit System Recovery
Search Open Websites/Domains (2)	User Execution (3)		Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Defense Evasion	Exploitation for Defense Evasion	Network Sniffing	File and Directory Permissions Modification (2)	Use Alternate Authentication Material (4)	Data from Local System	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 Share Discovery		Data from Removable Media	Non-Standard Port	Transfer Data to Cloud Account	Service Stop
			Windows Management Instrumentation	Process Injection (11)	Indicator Removal on Host (6)	Indicator Removal on Host (6)	Steal Web Session Cookie	Network Sniffing		Data Staged (2)	Protocol Tunneling		System Shutdown/Reboot
				Scheduled Task/Job (7)	Indirect Command Execution	Indirect Command Execution	Steal Kerberos Tickets (4)	Network Sniffing		Email Collection (3)	Proxy (4)		
				Valid Accounts (4)	Masquerading (6)	Masquerading (6)	Permission Groups Discovery (3)	Network Sniffing		Input Capture (4)	Remote Access Software		
					Modify Authentication Process (4)	Modify Authentication Process (4)	Process Discovery	OS Credential Dumping (8)		Man in the Browser	Traffic Signaling (1)		
					Modify Cloud Compute Infrastructure (4)	Modify Cloud Compute Infrastructure (4)	Query Registry	Steal Application Access Token		Man-in-the-Middle (2)	Web Service (3)		
					Modify Registry	Modify Registry	Remote System Discovery	Steal Web Session Cookie		Screen Capture			
					Modify System Image (2)	Modify System Image (2)	Software Discovery (1)	Two-Factor Authentication Interception		Video Capture			
					Network Boundary	Network Boundary	System Information Discovery	Unsecured Credentials (7)					
							System Location Discovery						
							System Network Configuration						

# «Методика оценки угроз безопасности информации»

Угроза несанкционированного доступа к базе данных, содержащей защищаемую информацию





# 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

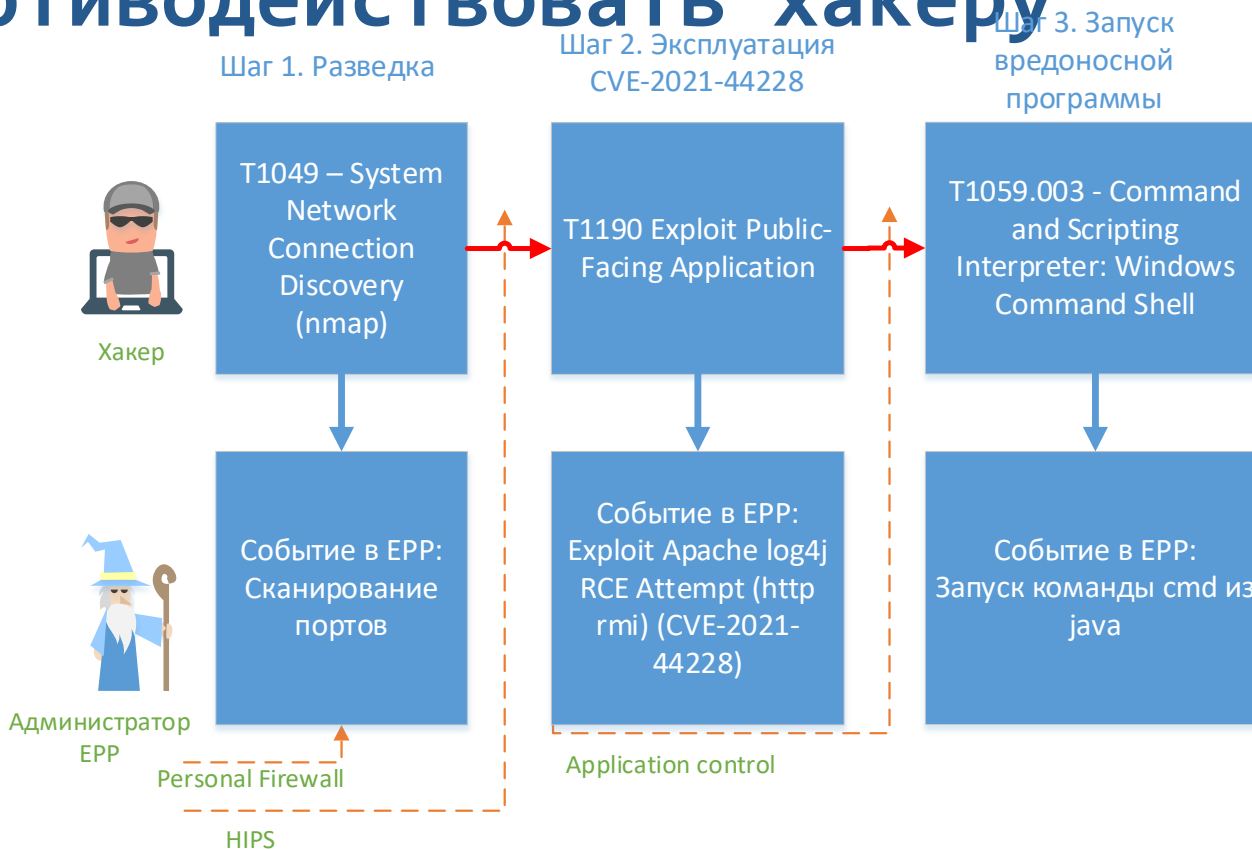


# Защита от внешних нарушителей и угроз

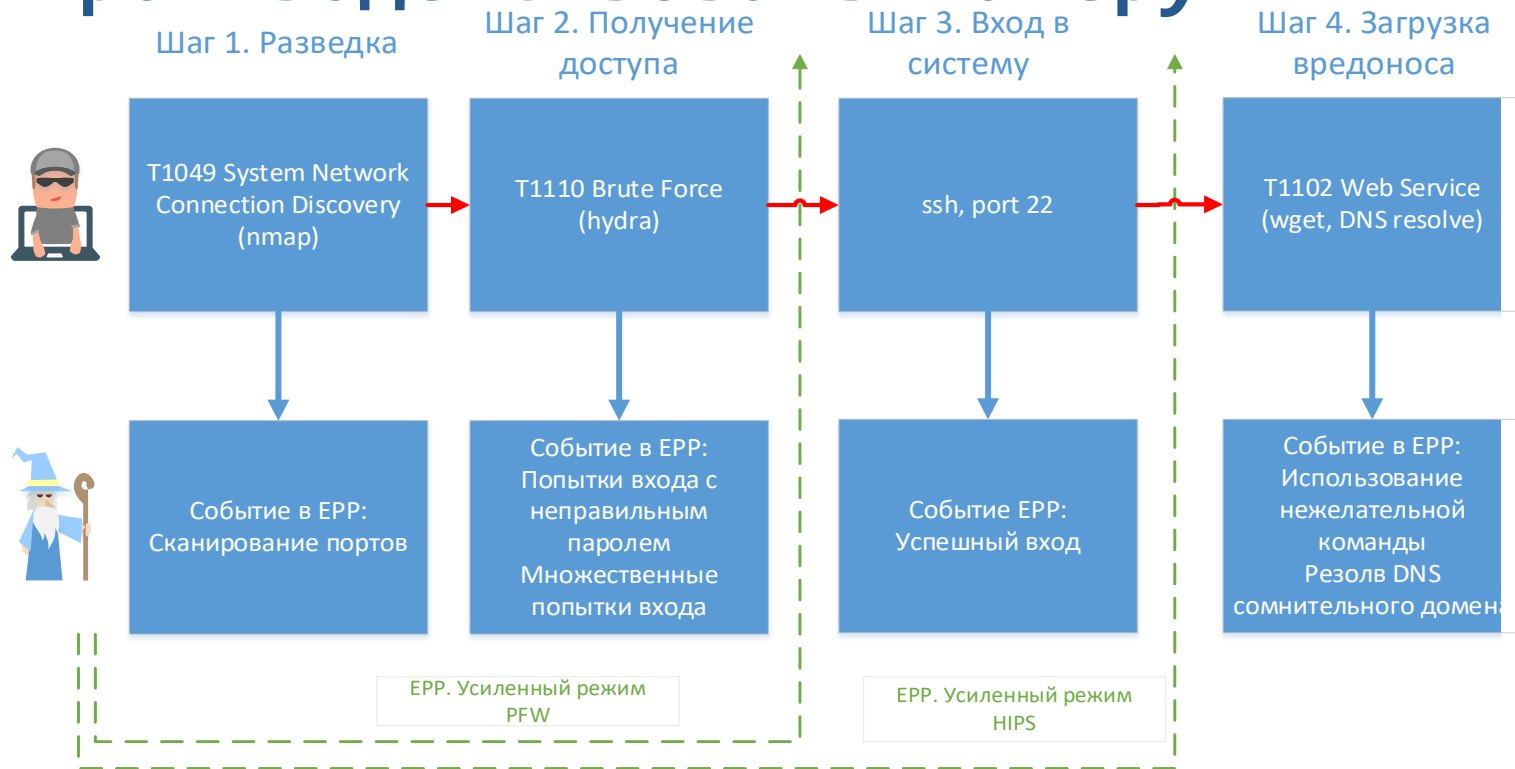
- Мониторинг и противодействие подозрительной активности на хосте
- Защита и предотвращение сетевых атак
- Защита от внедрения и выполнения вредоносных программ и кода
- Защита легитимных процессов



# 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

## Архитектура 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

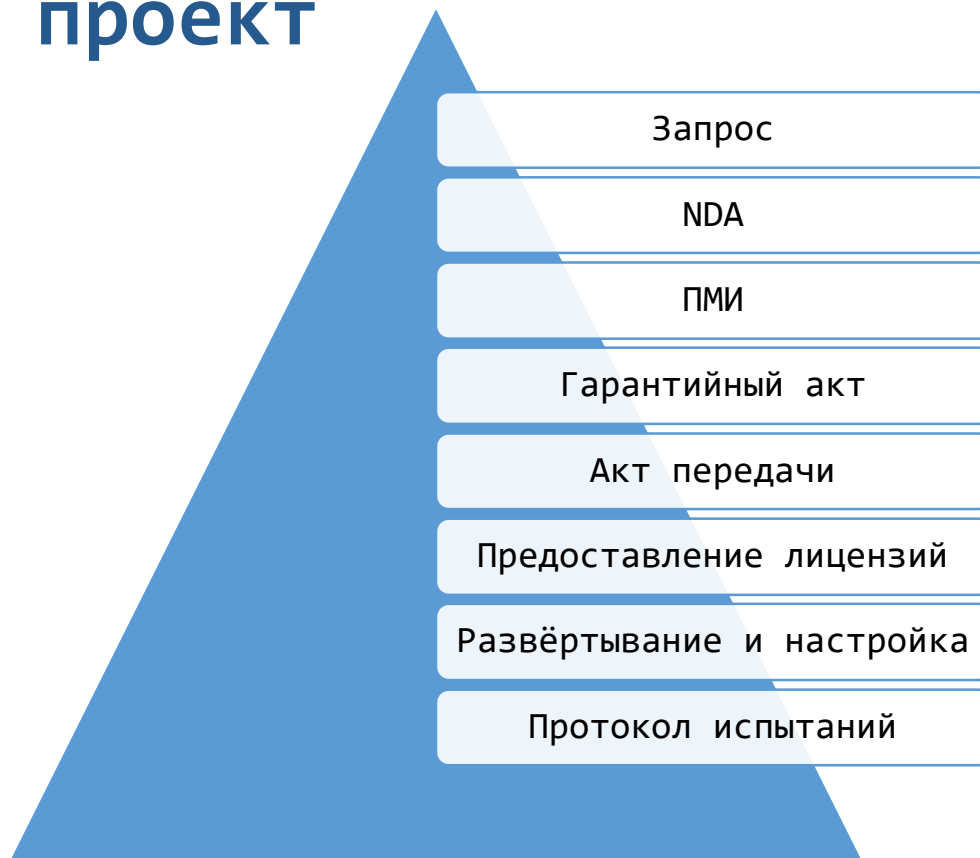
- **определяются субъекты доступа** (пользователи, процессы и иные субъекты доступа) и объекты доступа;
- **определяются политики управления доступом** (дискреционная, мандатная, ролевая, комбинированная);
- **определяются и обосновываются организационные и технические меры**, подлежащие реализации в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







**infotecs**

Спасибо  
за внимание!

Селифанов Валентин  
[Valentin.Selifanov@infotecs.ru](mailto:Valentin.Selifanov@infotecs.ru)

---

Подписывайтесь на наши соцсети

---



[vk.com/infotecs\\_news](https://vk.com/infotecs_news)



[https://t.me/infotecs\\_official](https://t.me/infotecs_official)



[rutube.ru/channel/24686363](https://rutube.ru/channel/24686363)