

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Управление рисками на практике

Николай Казанцев
ООО «НТФФ «ПОЛИСАН»



Риск информационной безопасности

— это вероятность того, что угрозы будут реализовываться с использованием уязвимостей информационных активов или групп информационных активов и, тем самым, наносить ущерб организации.

ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems Overview and vocabulary

#CODEIB

УГРОЗА

+

УЯЗВИМОСТЬ

+

АКТИВ

Что то плохое
и понятное
ВСЕМ

Любое свойство актива,
даже факт его
существования
! не CVE

Все что угодно

БАЗЫ ЗНАНИЙ



MITRE | ATT&CK®

bdu.fstec.ru

attack.mitre.org



capec.mitre.org



owasp.org



cwe.mitre.org



Банк данных угроз безопасности информации

Федеральная служба по техническому и экспортному контролю

ФСТЭК России

Государственный научно-исследовательский испытательный институт проблем технической защиты информации

ФАУ «ГНИИИ ПТЗИ ФСТЭК России»



Угрозы Уязвимости ▾ Документы ▾ Термины Обратная связь ▾ Обновления ▾ Участники ▾ ФСТЭК России

Поиск



Главная / Список угроз

ФИЛЬТРАЦИЯ

Контекстный поиск по названию угрозы



Введите слово или словосочетание

Источник угрозы ⓘ

Выводить по: 10, 20, 50, 100

Элементы с 1 по 10 из 217

УБИ. 001 Угроза автоматического распространения вредоносного кода в грид-системе

УБИ. 002 Угроза агрегирования данных, передаваемых в грид-системе

УГРОЗА ? РИСК

УБИ. 004 Угроза аппаратного сброса пароля BIOS

УБИ. 005 Угроза внедрения вредоносного кода в BIOS

УБИ. 006 Угроза внедрения кода или данных

УБИ. 007 Угроза воздействия на программы с высокими привилегиями

УБИ. 008 Угроза восстановления и/или повторного использования аутентификационной информации

УБИ. 009

ПОСЛЕДНИЕ ИЗМЕНЕНИЯ

11.02.2020

УБИ. 217 Угроза использования скомпрометированного доверенного источника обновлений программного

Нарушение конфиденциальности

Нарушение целостности

Нарушение доступности

Сброс

Применить

приложениям, установленным на Smart-картах

15.11.2019

УБИ. 215 Угроза несанкционированного доступа к системе при помощи сторонних сервисов

15.11.2019

УБИ. 214 Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации

УБИ.198: Угроза скрытной регистрации вредоносной программой учетных записей администраторов

Описание угрозы Угроза заключается в возможности скрытного создания внедренной вредоносной программой учетных записей с правами администратора с целью последующего их использования для несанкционированного доступа к пользовательской информации и к настройкам программного обеспечения, установленного на инфицированном компьютере.

Данная угроза обусловлена недостаточностью мер по антивирусной защите, что позволяет выполнить неконтролируемый запуск вредоносного программного обеспечения (отсутствие контроля разрешенного программного обеспечения).

Кроме того, данная угроза обусловлена недостаточностью мер по разграничению доступа (контроль создания учетных записей пользователей).

Реализация данной угрозы возможна при условии, что на атакуемом компьютере открыт RDP-порт

Источники угрозы ? Внешний нарушитель со средним потенциалом

Объект воздействия Система управления доступом, встроенная в операционную систему компьютера (программное обеспечение)

Последствия реализации угрозы Нарушение целостности

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	Command and Scripting Interpreter (7)	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	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (11)	Boot or Logon Autostart Execution (11)	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
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Service Session Hijacking (2)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Phishing (3)	Scheduled Task/Job (5)	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Direct Volume Access	Input Capture (4)	Cloud Service Discovery	Remote Services (6)	Data from Cloud Storage Object	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Replication Through Removable Media	Shared Modules	Browser Extensions	Create or Modify System Process (4)	Execution Guardrails (1)	Man-in-the-Middle (1)	Domain Trust Discovery	Replication Through Removable Media	Data from Information Repositories (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Supply Chain Compromise (3)	Software Deployment Tools	Compromise Client Software Binary	Event Triggered Execution (15)	Exploitation for Defense Evasion	Modify Authentication Process (3)	File and Directory Discovery	Software Deployment Tools	Data from Local System	Fallback Channels	Exfiltration Over Other Network Medium (1)	Endpoint Denial of Service (4)
Trusted Relationship	System Services (2)	Create Account (3)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Network Sniffing	Network Service Scanning	Taint Shared Content	Data from Network Shared Drive	Ingress Tool Transfer	Exfiltration Over Physical Medium (1)	Firmware Corruption
Valid Accounts (4)	User Execution (2)	Create or Modify System Process (4)	Group Policy Modification	Group Policy Modification	OS Credential Dumping (8)	Network Share Discovery	Use Alternate Authentication Material (4)	Data from Network Shared Drive	Multi-Stage Channels	Exfiltration Over Web Service (2)	Inhibit System Recovery
	Windows Management Instrumentation	Event Triggered Execution (15)	Hide Artifacts (6)	Hide Artifacts (6)	Steal Application Access Token	Network Sniffing		Data from Removable Media	Non-Application Layer Protocol	Scheduled Transfer	Network Denial of Service (2)
		External Remote Services	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (3)	Password Policy Discovery		Data Staged (2)	Non-Standard Port	Transfer Data to Cloud Account	Resource Hijacking
		Hijack Execution Flow (11)	Impair Defenses (6)	Impair Defenses (6)	Steal Web Session Cookie	Peripheral Device Discovery		Email Collection (3)	Protocol Tunneling	Service Stop	System Shutdown/Reboot
		Implant Container Image	Indicator Removal on Host (6)	Indicator Removal on Host (6)	Two-Factor Authentication Interception	Permission Groups Discovery (3)		Input Capture (4)	Proxy (4)		
		Office Application Startup (6)	Indirect Command Execution	Indirect Command Execution	Unsecured Credentials (6)	Process Discovery		Man in the Browser	Remote Access Software		
		Pre-OS Boot (3)	Masquerading (6)	Masquerading (6)		Query Registry		Man-in-the-Middle (1)	Traffic Signaling (1)		
		Scheduled Task/Job (5)	Modify Authentication Process (3)	Modify Authentication Process (3)		Remote System Discovery		Screen Capture	Web Service (3)		
		Server Software Component (3)	Modify Cloud Compute Infrastructure (4)	Modify Cloud Compute Infrastructure (4)		Software Discovery (1)		Video Capture			
		Traffic Signaling (1)	Modify Registry	Modify Registry		System Information Discovery					
		Valid Accounts (4)	Obfuscated Files or Information (5)	Obfuscated Files or Information (5)		System Network Configuration Discovery					
			Pre-OS Boot (3)	Pre-OS Boot (3)		System Network Connections Discovery					
			Process Injection (11)	Process Injection (11)		System Owner/User Discovery					
			Rogue Domain Controller	Rogue Domain Controller		System Service Discovery					
						System Time Discovery					

Create Account: Local Account

Other sub-techniques of Create Account (3) ▼

Adversaries **may create a local account** to maintain access to victim systems. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service. With a sufficient level of access, the `net user /add` command can be used to create a local account.

Such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system.

ID: T1136.001

Sub-technique of: [T1136](#)

Tactic: **Persistence**

Platforms: **Linux, Windows, macOS**

Permissions

Required: Administrator

Data Sources: Authentication logs, Process command-line parameters, Process monitoring, Windows event logs

Version: 1.0

Created: 28 January 2020

Last Modified: 23 March 2020

Формирование рисков

из-за

в

УГРОЗА

- Закрепление злоумышленника в инфраструктуре

УЯЗВИМОСТИ

- Возможность создания локальных учетных записей

АКТИВ

- Операционная система



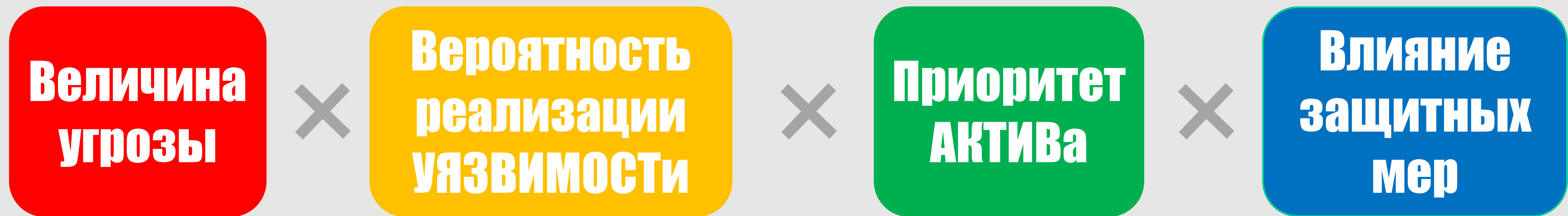
УБИ.198

АТТ&СК®

T1136.001

Оценка рисков

FAIR, FRAP, OCTAVE ...

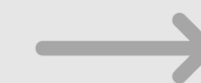


Критерии
оценки



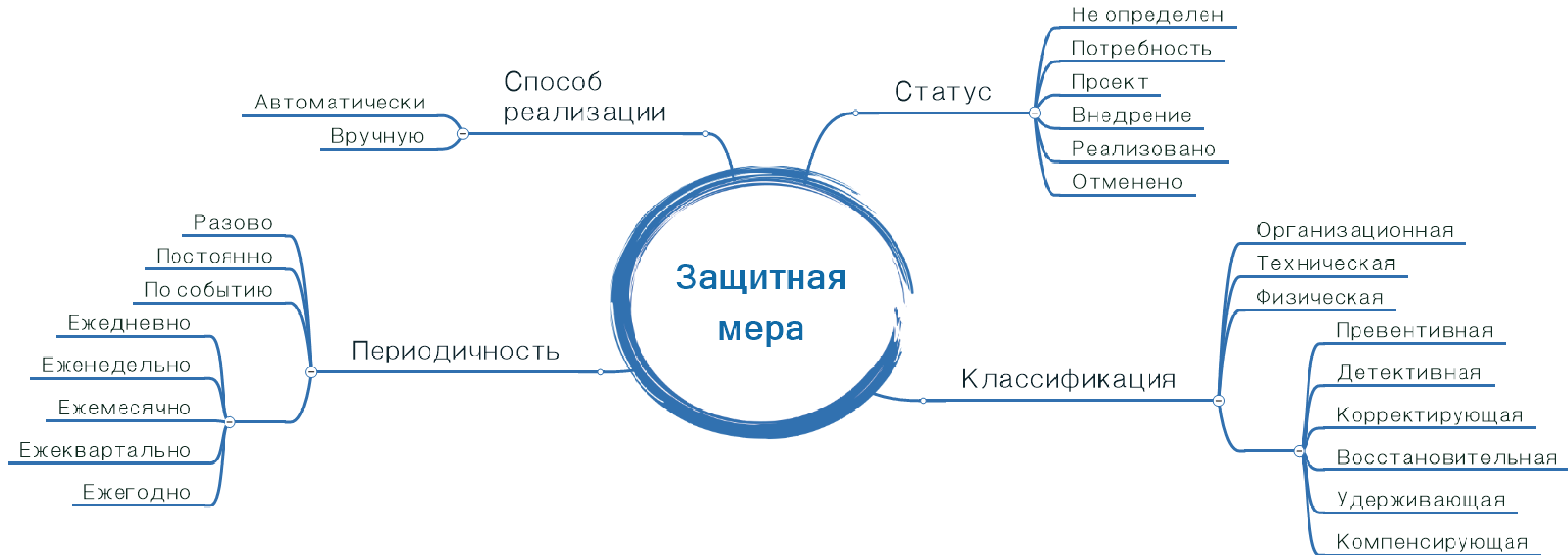
Качественная
оценка

- 0 – Отсутствует
- 1 – Низкий
- 2 – Средний
- 3 – Высокий
- 4 – Критический



Снижение вероятности
Снижение величины
угрозы

Защитные меры



Карточка защитной меры

МЕРА

- Обнаружение несанкционированных учетных записей пользователей и администраторов на ПК

СТАТУС

- Реализовано
- 17.10.2017

РЕАЛИЗАЦИЯ

- Автоматически

ПЕРИОДИЧНОСТЬ

- Ежедневно

ТИП

- Техническая
- Детективная

ИНСТРУМЕНТЫ

- SIEM

ОТВЕТСТВЕННЫЙ

- Отдел ИБ

План обработки рисков

Риск	Защитные меры	Первичный риск	Текущий риск	Остаточный риск
Угроза Закрепление злоумышленника в инфраструктуре из-за уязвимости Возможность создания локальных учетных записей в Активе Операционная система	Проект : ➤ Автоматическое удаление несанкционированных локальных учетных записей на ПК Реализовано : ➤ Разовая инвентаризация и удаление локальных администраторов на ПК ➤ Автоматическая смена паролей локальных администраторов на ПК (MS LAPS) ➤ Обнаружение несанкционированных учетных записей пользователей и членов групп администраторов на ПК	18 - Высокий	8.75 - Средний	5.25 - Низкий

Метрики

Интегральный риск



История снижения рисков

Классификация рисков



Оценка рисков в контексте БДУ ФСТЭК

БДУ №	Название	Связанные риски	Риск
139	Угроза преодоления физической защиты	1 1	8.4 - Средний
4	Угроза аппаратного сброса пароля BIOS	1 1	8 - Средний
111	Угроза передачи данных по скрытым каналам	1 1	7.6 - Средний
8	Угроза восстановления аутентификационной информации	4 0	6.155 - Низкий
91	Угроза несанкционированного удаления защищаемой информации	1 0	4.8 - Низкий
60	Угроза неконтролируемого уничтожения информации хранилищем больших данных	1 0	4.8 - Низкий
43	Угроза нарушения доступности облачного сервера	1 0	4 - Низкий

Принципы

1 УЧЕТ МЕР

Не начинаем внедрение пока защитная мера не учтена

2 УЧЕТ РИСКОВ ДЛЯ КАЖДОЙ МЕРЫ

Каждая защитная мера должна быть ответом на риски

3 ПОНЯТНЫЕ УГРОЗЫ

Угрозы должны быть просты и понятны не только ИТ/ИБ

4 ДИНАМИКА

Вместо планового подхода - непрерывная работа

PROFIT

Единая система управления
информационной
безопасностью
на стратегическом
и тактическом уровнях



Знаем ЧТО важно и ПОЧЕМУ



Можем это показать и доказать



**Экономим и обосновываем
затраты**



Разделяем ответственность

— #CODEIB —

СПАСИБО ЗА ВНИМАНИЕ



+7 906 255 2009

t.me/NicKazantsev

spbsecurity.blogspot.com



**КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ**