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

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»

ФИЛЬТРАЦИЯ

Контекстный поиск по названию угрозы

Введите слово или словосочетание

Источник угрозы

Нарушение конфиденциальности

Нарушение целостности

Нарушение доступности

Сброс | Применить

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
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

ПОСЛЕДНИЕ ИЗМЕНЕНИЯ

11.02.2020

УБИ. 217 Угроза использования скомпрометированного доверенного источника обновлений программного

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

MITRE | ATT&CK®

Adversarial Tactics, Techniques and Common Knowledge

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	УЯЗВИМОСТи	АКТИВе
• Закрепление • злоумышленника • в инфраструктуре	• Возможность создания • локальных учетных • записей	• Операционная система

УБИ.198

ATT&CK®

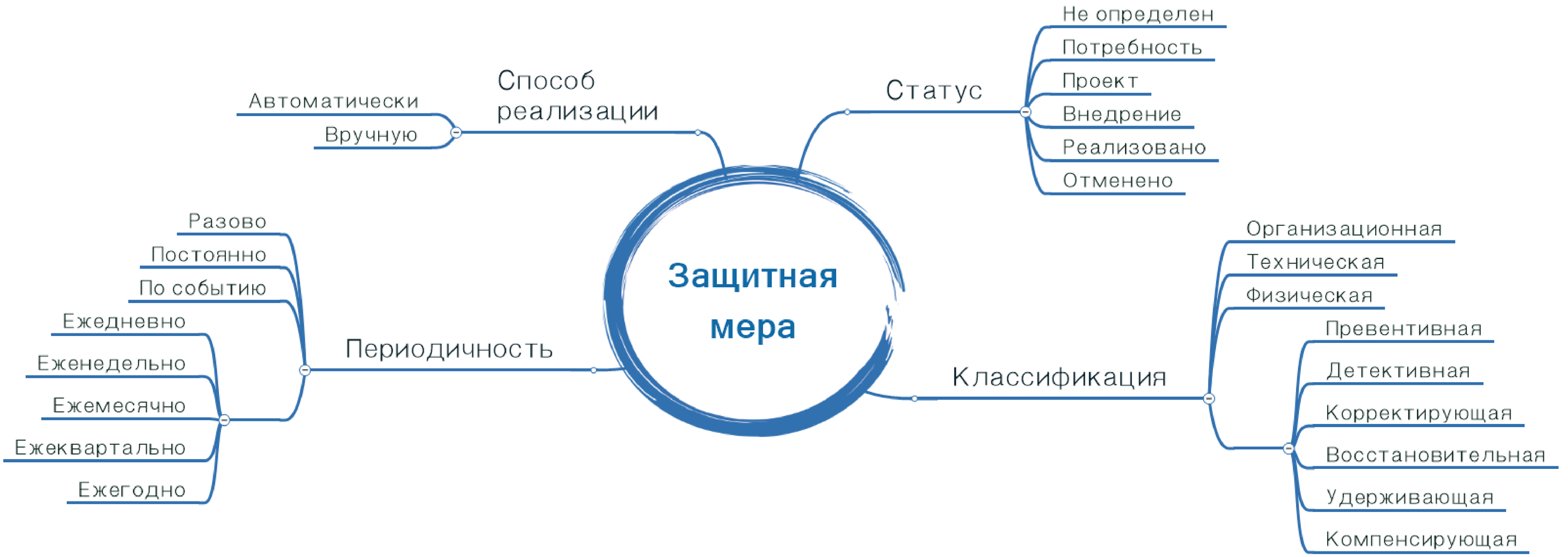
T1136.001

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