Основы информационной безопасности. Обучение в записи

Урок 4. Семинар: Моделирование угроз и выбор мер защиты

Оглавление

Задание 1

Задание №1

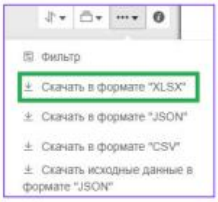
- Вам как ИБ-специалисту компании «Самый лучший образовательный сайт» пришла пора смоделировать угрозы безопасности информации для вашей информационной системы:
- Какие свойства информации (данных) вам необходимо обеспечить?
- Какие актуальные способы реализации угроз для вашей информационной системы?

Семинар 2. Моделирование угроз и выбор мер защиты

Задание №1 (инструкция)

Шаги:

- Выбрать негативные последствия.
- Выбрать угрозы (свойства информации).
- Выбрать объекты воздействия.
- Выбрать компоненты объектов воздействия.
- Выбрать возможности нарушителя.
- Скачать файл в XLSX-формате.



Выберите негативные последствия

- [ ] Н.1 Угроза жизни или здоровью.
- [ ] Н.2 Нарушение неприкосновенности частной жизни.
- [ ] Н.3 Нарушение личной, семейной тайны, утрата чести и доброго имени.
- [ ] Н.4 Нарушение тайны переписки, телефонных переговоров, иных сообщений.
- [ ] Н.5 Нарушение иных прав и свобод гражданина, закрепленные в Конституции Российской Федерации и федеральных законах.
- [ ] Н.6 Финансовый, иной материальный ущерб физического лица.
- [x] Н.7 Нарушение конфиденциальности (утечка) персональных данных.
- [ ] Н.8 Разглашение персональных данных граждан.
- [x] Н.30 Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.).
- [ ] Н.31 Причинение ущерба жизни и здоровью людей.
- [ ] Н.32 Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения.
- [x] Н.51 Утечка информации ограниченного доступа.
- [ ] Н.52 Непредставление государственных услуг.

Назад | Далее

Выберите угрозы

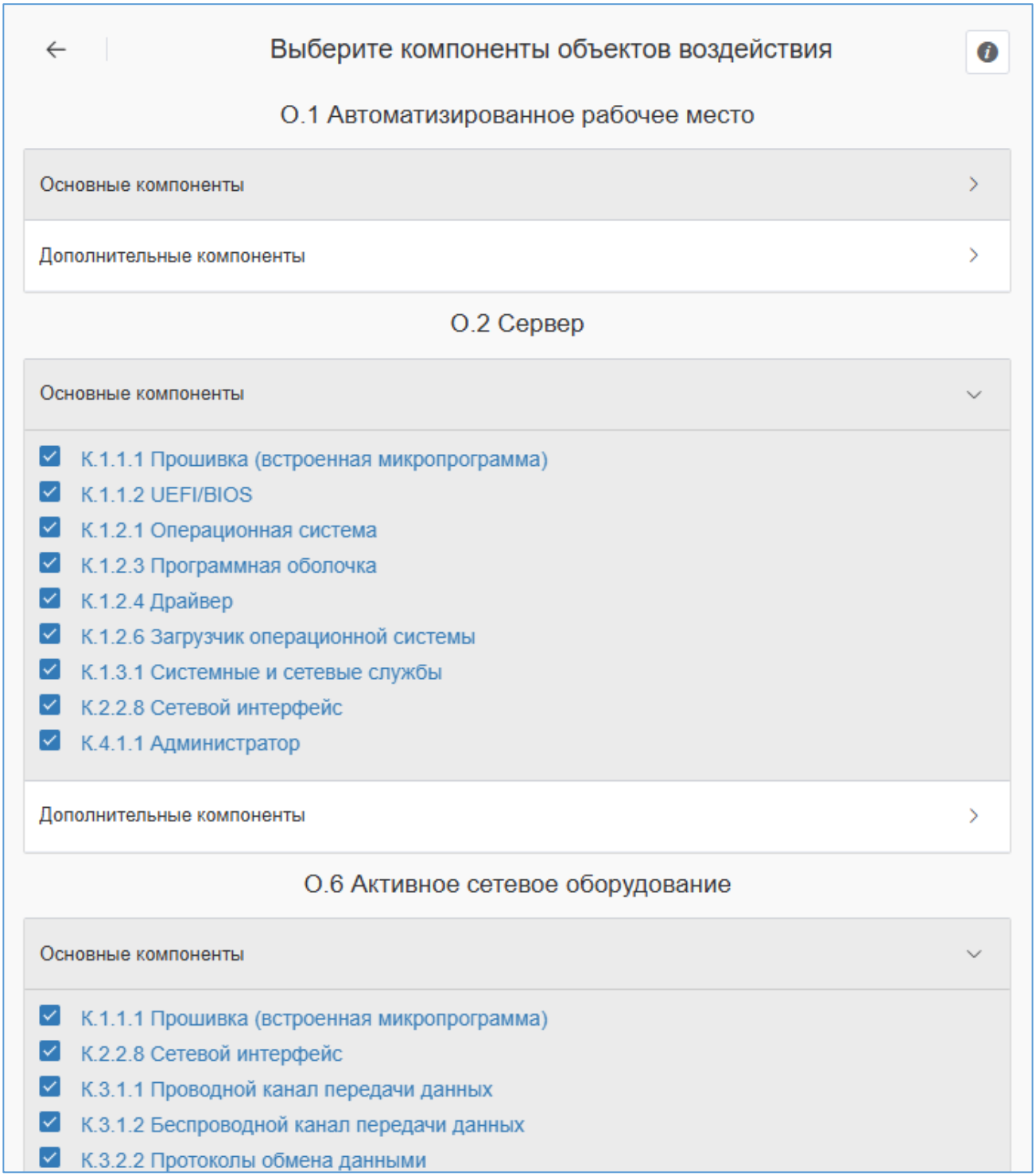
- [x] УБИ.1 Угроза утечки информации
- [x] УБИ.2 Угроза несанкционированного доступа
- [x] УБИ.3 Угроза несанкционированной модификации (искажения)
- [x] УБИ.4 Угроза несанкционированной подмены
- [ ] УБИ.5 Угроза удаления информационных ресурсов
- [ ] УБИ.6 Угроза отказа в обслуживании
- [ ] УБИ.7 Угроза ненадлежащего (нецелевого) использования
- [x] УБИ.8 Угроза нарушения функционирования (работоспособности)
- [ ] УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника
- [ ] УБИ.10 Угроза распространения противоправной информации
- [x] УБИ.11 Угроза несанкционированного массового сбора информации

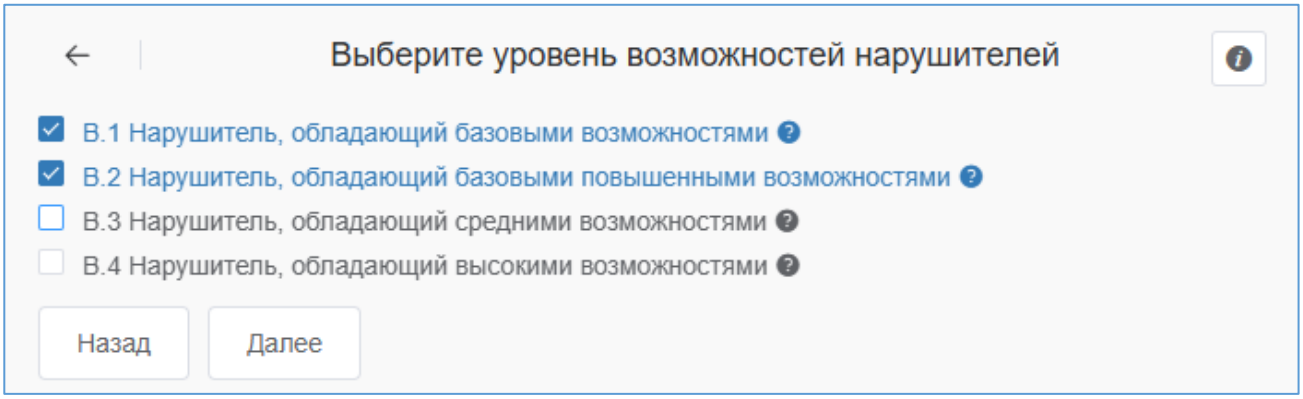
Назад | Далее

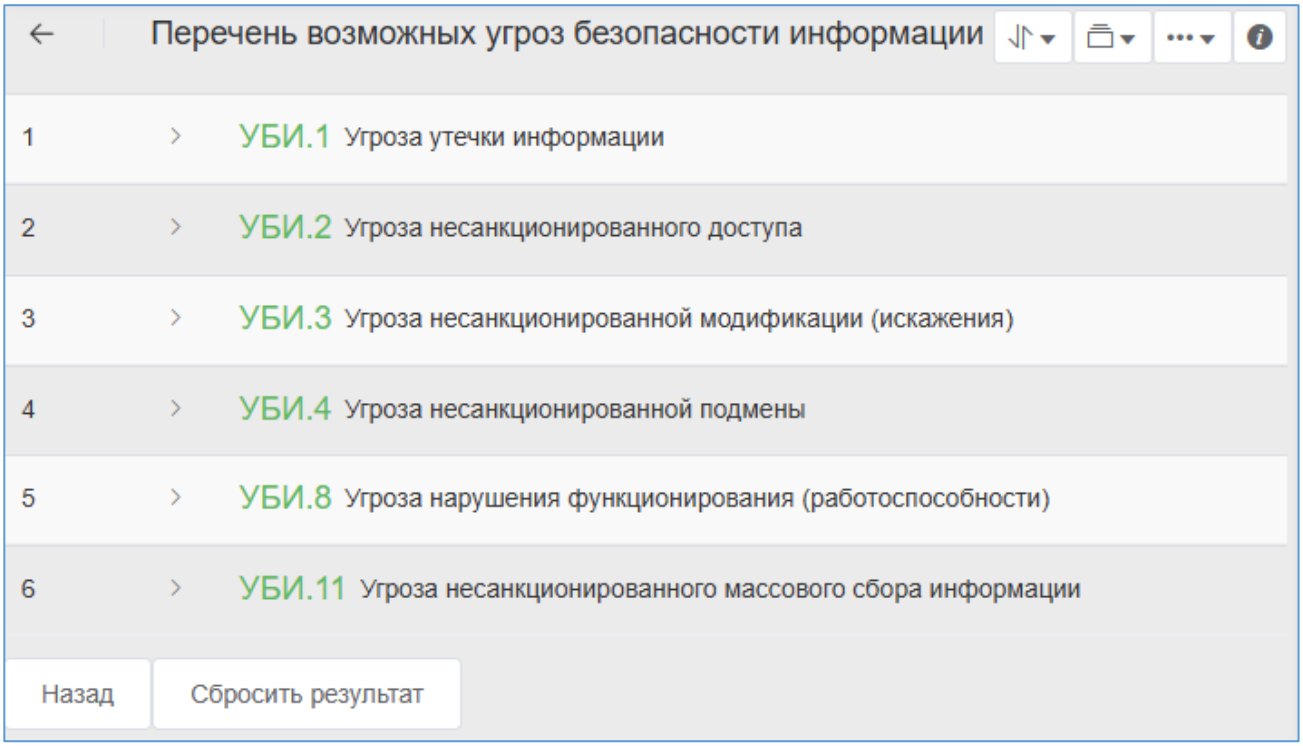
Выберите объекты воздействия

- [x] О.1 Автоматизированное рабочее место
- [x] О.2 Сервер
- [ ] О.3 Периферийное оборудование
- [ ] О.4 Устройство хранения данных
- [ ] О.5 Устройство интернета-вещей
- [x] О.6 Активное сетевое оборудование
- [ ] О.7 Обеспечивающие системы
- [ ] О.8 Телефония (VoIP, GSM)
- [x] О.9 Средства защиты информации
- [ ] О.10 Мобильное устройство
- [ ] О.12 Физические линии связи

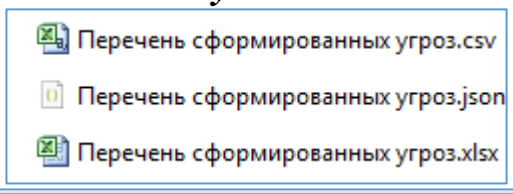
Назад | Далее


Выберите компоненты объектов воздействия
О.1 Автоматизированное рабочее место
Основные компоненты
Дополнительные компоненты
О.2 Сервер
Основные компоненты
К.1.1.1 Прошивка (встроенная микропрограмма)
К.1.1.2 UEFI/BIOS
К.1.2.1 Операционная система
К.1.2.3 Программная оболочка
К.1.2.4 Драйвер
К.1.2.6 Загрузчик операционной системы
К.1.3.1 Системные и сетевые службы
К.2.2.8 Сетевой интерфейс
К.4.1.1 Администратор
Дополнительные компоненты
О.6 Активное сетевое оборудование
Основные компоненты
К.1.1.1 Прошивка (встроенная микропрограмма)
К.2.2.8 Сетевой интерфейс
К.3.1.1 Проводной канал передачи данных
К.3.1.2 Беспроводной канал передачи данных
К.3.2.2 Протоколы обмена данными


Выберите уровень возможностей нарушителей
В.1 Нарушитель, обладающий базовыми возможностями
В.2 Нарушитель, обладающий базовыми повышенными возможностями
В.3 Нарушитель, обладающий средними возможностями
В.4 Нарушитель, обладающий высокими возможностями
Назад
Далее



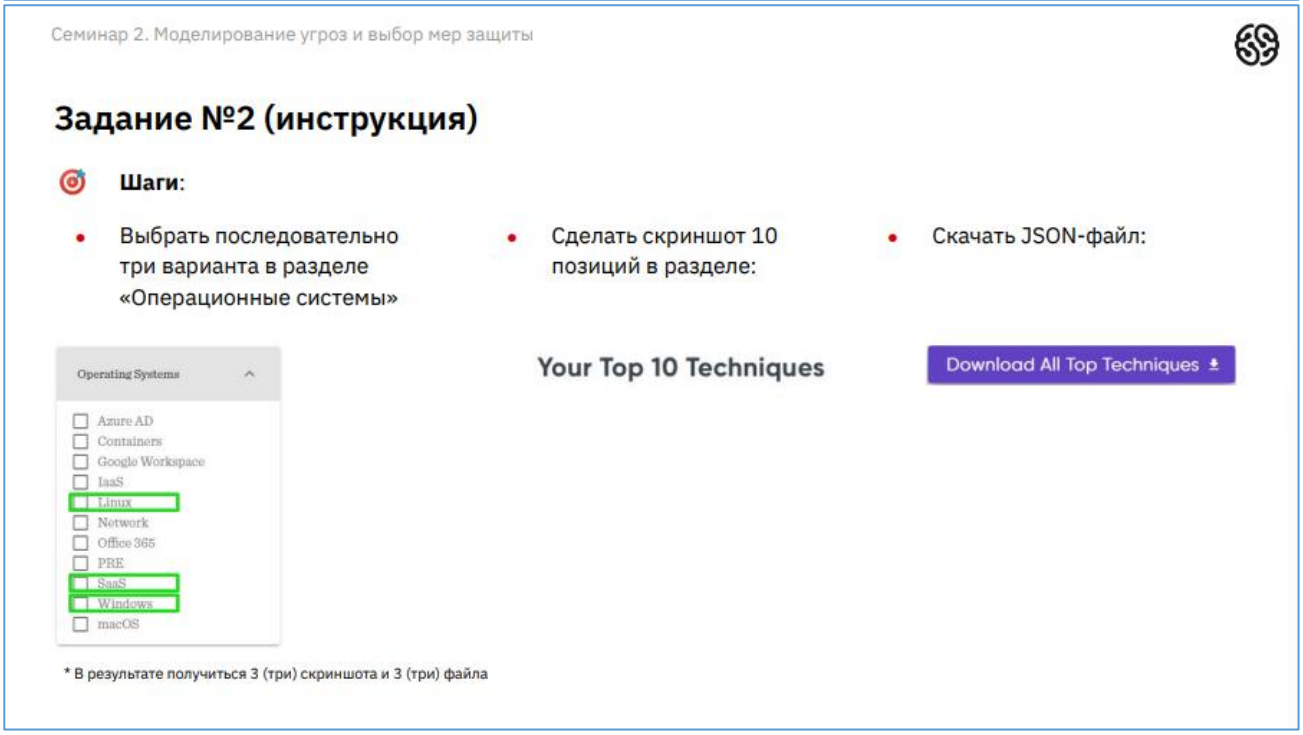
Результат:



	A	B	C	D	E	F	G	H
1	Идентификатор	Наименов	Описание	Объект во	Компонен	Способы реализации	Потенциал нарушителя	Меры защиты
2	УБИ.1.1.1	Угроза уте	Угроза зак	О.1 Автом	К.1.1.1 Пр	СП.1.1 Эксплуатация известных уязвимостей;СП.1.2 Экс	В.1 Нарушитель, обладак	АУД.2.1 Выявление (пои
3	УБИ.1.1.2	Угроза уте	Угроза зак	О.1 Автом	К.1.1.1 Пр	СП.2.1 Использование недостатков, связанных с неполн	В.1 Нарушитель, обладак	АУД.1.3 Контроль выпол
4	УБИ.1.1.3	Угроза уте	Угроза зак	О.1 Автом	К.1.1.1 Пр	СП.3.1 Эксплуатация недостатков незащищенных прото	В.1 Нарушитель, обладак	ЗИС.19.1 Защита информ
5	УБИ.1.1.4	Угроза уте	Угроза зак	О.1 Автом	К.1.1.1 Пр	СП.4.1 Внедрение вредоносного программного обеспеч	В.1 Нарушитель, обладак	АВЗ.1.1 Применение сре
6	УБИ.1.1.5	Угроза уте	Угроза зак	О.1 Автом	К.1.5.11 П	СП.5.1 Внедрение закладок в прикладное программное	В.2 Нарушитель, обладак	ЗНИ.5.1 Определение ог
7	УБИ.1.1.7	Угроза уте	Угроза зак	О.1 Автом	К.2.2.8 Сет	СП.7.1 Прослушивание интерфейсов сети	В.1 Нарушитель, обладак	ЗИС.2.2 Обеспечение вз
8	УБИ.1.1.8	Угроза уте	Угроза зак	О.1 Автом	К.1.2.1 Оп	СП.8.5 Идентификация пользователей;СП.8.6 Обнаруже	В.1 Нарушитель, обладак	АУД.5.1 Применение сис
9	УБИ.1.1.9	Угроза уте	Угроза зак	О.1 Автом	К.1.2.1 Оп	СП.9.6 Поиск файлов и каталогов	В.2 Нарушитель, обладак	АУД.5.1 Применение сис
10	УБИ.1.1.10	Угроза уте	Угроза зак	О.1 Автом	К.1.1.1 Пр	СП.10.7 Атаки на уровне каналов и сети, приводящие к	В.2 Нарушитель, обладак	ЗИС.27.1 Обеспечение п
11	УБИ.1.1.12	Угроза уте	Угроза зак	О.1 Автом	К.1.2.1 Оп	СП.12.1 Считывание нажатий клавиш на клавиатуре;СП	В.1 Нарушитель, обладак	АВЗ.1.1 Применение сре
12	УБИ.1.1.13	Угроза уте	Угроза зак	О.1 Автом	К.4.1.1 Ад	СП.13.1 Целенаправленная рассылка через рассылку ре	В.1 Нарушитель, обладак	АВЗ.1.1 Применение сре
13	УБИ.1.1.18	Угроза уте	Угроза зак	О.1 Автом	К.1.1.1 Пр	СП.18.1 Доступ без авторизации;СП.18.2 Использование	В.1 Нарушитель, обладак	ИАФ.1.1 Аутентификация
14	УБИ.1.1.24	Угроза уте	Угроза зак	О.1 Автом	К.2.1.2 Мо	СП.24.2 Внесение изменений в конфигурацию на уровн	В.1 Нарушитель, обладак	ЗТС.2.1 Обеспечение ко
15	УБИ.1.1.25	Угроза уте	Угроза зак	О.1 Автом	К.1.2.1 Оп	СП.25.1 Атаки на механизмы идентификации участнико	В.1 Нарушитель, обладак	АУД.2.1 Выявление (пои
16	УБИ.1.1.26	Угроза уте	Угроза зак	О.1 Автом	К.1.3.1 Си	СП.26.5 Внедрение вредоносного ПО через компромета	В.1 Нарушитель, обладак	АВЗ.1.1 Применение сре
17	УБИ.1.2.1	Угроза уте	Угроза зак	О.2 Серве	К.1.1.1 Пр	СП.1.1 Эксплуатация известных уязвимостей;СП.1.2 Экс	В.1 Нарушитель, обладак	АУД.2.1 Выявление (пои

Задание 2


Семинар 2. Моделирование угроз и выбор мер защиты
Задание №2
Вы дополнительно решили определить актуальные техники атакующих для вашей информационной системы.
Клиентские данные (веб-браузер, оперативная память)
Запросы и ответы (сетевой трафик)
Данные веб-сайта (front)
Табличные данные (back)
Файловые данные (архив)
Клиент
Сеть Интернет
Веб-сайт интернет
База данных
Резервные копии
get
select
export
Используемые данные
Данные в движении
Используемые данные
Используемые данные. Данные в покое
Данные в покое


Семинар 2. Моделирование угроз и выбор мер защиты
Задание №2 (инструкция)
Шаги:
Выбрать последовательно три варианта в разделе «Операционные системы»
Сделать скриншот 10 позиций в разделе:
Скачать JSON-файл:
Operating Systems
Azure AD
Containers
Google Workspace
IaaS
Linux
Network
Office 365
PRE
SaaS
Windows
macOS
Your Top 10 Techniques
Download All Top Techniques
* В результате получиться 3 (три) скриншота и 3 (три) файла

TOP ATT&CK TECHNIQUES CALCULATOR

Select the filters and/or components below, then click Generate to see a customized ranking of ATT&CK techniques.

FILTERS

- NIST 800-53 CONTROLS
- CIS SECURITY CONTROLS
- DETECTION ANALYTICS
- OPERATING SYSTEMS

- [ ] All OS Controls
- [ ] Azure AD
- [ ] Containers
- [ ] Google Workspace
- [ ] IaaS
- [x] Linux
- [ ] macOS
- [ ] Network
- [ ] Office 365
- [ ] PRE
- [ ] SaaS
- [ ] Windows

SCORE YOUR SYSTEM

NETWORK MONITORING COMPONENTS	NONE / LOW / MEDIUM / HIGH
PROCESS MONITORING COMPONENTS	NONE / LOW / MEDIUM / HIGH
FILE MONITORING COMPONENTS	NONE / LOW / MEDIUM / HIGH
CLOUD MONITORING COMPONENTS	NONE / LOW / MEDIUM / HIGH
HARDWARE MONITORING COMPONENTS	NONE / LOW / MEDIUM / HIGH

GENERATE

YOUR TOP 10 TECHNIQUES

NO NETWORK MONITORING | NO PROCESS MONITORING | NO FILE MONITORING | NO CLOUD MONITORING | NO HARDWARE MONITORING | NIST: ALL NIST CONTROLS | CIS: ALL CIS CONTROLS | DETECTION: ALL DETECTION CONTROLS | OS: LINUX EDIT SELECTION

1. T1562 IMPAIR DEFENSES
2. T1059 COMMAND AND SCRIPTING INTERPRETER
3. T1053 SCHEDULED TASK/JOB
4. T1218 SYSTEM BINARY PROXY EXECUTION
5. T1543 CREATE OR MODIFY SYSTEM PROCESS
6. T1055 PROCESS INJECTION
7. T1036 MASQUERADING
8. T1574 HIJACK EXECUTION FLOW
9. T1021 REMOTE SERVICES
10. T1204 USER EXECUTION

DOWNLOAD

T1562 IMPAIR DEFENSES

DESCRIPTION

Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators.

Adversaries may also impair routine operations that contribute to defensive hygiene, such as blocking users from logging out of a computer or stopping it from being shut down. These restrictions can further enable malicious operations as well as the continued propagation of incidents.(Citation: Emotet shutdown)

Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components.

SUBTECHNIQUES

- T1562.001 DISABLE OR MODIFY TOOLS
- T1562.002 DISABLE WINDOWS EVENT LOGGING
- T1562.003 IMPAIR COMMAND HISTORY LOGGING
- T1562.004 DISABLE OR MODIFY SYSTEM FIREWALL
- T1562.006 INDICATOR BLOCKING
- T1562.007 DISABLE OR MODIFY CLOUD FIREWALL

Linux.json 9+, U

C: > Users > user > Desktop > GeekBrains-specialization-ELECTIVES > 13. Fundamentals of Information Security > Seminar-02 > TopTenTechniques > {} Linux.json > {} 0 > [ ] mitigations > {} 1


```
[
    {
        "rank": 1,
        "tid": "T1562",
        "name": "Impair Defenses",
        "description": "Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not
        "url": "https://attack.mitre.org/techniques/T1562",
        "detection": "Monitor processes and command-line arguments to see if security tools or logging services are killed or stop running. Monitor Registr
        "score": 3.6095241904761903,
        "mitigations": [
            {
                "mid": "M1047",
                "name": "Audit",
                "description": "Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential wea
                "url": "https://attack.mitre.org/mitigations/M1047"
            },
            {
                "mid": "M1038",
                "name": "Execution Prevention",
                "description": "Block execution of code on a system through application control, and/or script blocking.",
                "url": "https://attack.mitre.org/mitigations/M1038"
            },
            {
                "mid": "M1022",
                "name": "Restrict File and Directory Permissions",
```

TOP ATT&CK TECHNIQUES CALCULATOR

Select the filters and/or components below, then click Generate to see a customized ranking of ATT&CK techniques.

FILTERS

- NIST 800-53 CONTROLS
- CIS SECURITY CONTROLS
- DETECTION ANALYTICS
- OPERATING SYSTEMS
  - [ ] All OS Controls
  - [ ] Azure AD
  - [ ] Containers
  - [ ] Google Workspace
  - [ ] IaaS
  - [ ] Linux
  - [ ] macOS
  - [ ] Network
  - [ ] Office 365
  - [ ] PRE
  - [x] SaaS
  - [ ] Windows

SCORE YOUR SYSTEM

	NONE	LOW	MEDIUM	HIGH
NETWORK MONITORING COMPONENTS	NONE	LOW	MEDIUM	HIGH
PROCESS MONITORING COMPONENTS	NONE	LOW	MEDIUM	HIGH
FILE MONITORING COMPONENTS	NONE	LOW	MEDIUM	HIGH
CLOUD MONITORING COMPONENTS	NONE	LOW	MEDIUM	HIGH
HARDWARE MONITORING COMPONENTS	NONE	LOW	MEDIUM	HIGH

GENERATE

YOUR TOP 10 TECHNIQUES

NO NETWORK MONITORING | NO PROCESS MONITORING | NO FILE MONITORING | NO CLOUD MONITORING | NO HARDWARE MONITORING | NIST: ALL NIST CONTROLS | CIS: ALL CIS CONTROLS | DETECTION: ALL DETECTION CONTROLS | OS: SAAS | EDIT SELECTION

1. T1078 VALID ACCOUNTS
2. T1552 UNSECURED CREDENTIALS
3. T1110 BRUTE FORCE
4. T1546 EVENT TRIGGERED EXECUTION
5. T1098 ACCOUNT MANIPULATION
6. T1136 CREATE ACCOUNT
7. T1048 EXFILTRATION OVER ALTERNATIVE PROTOCOL
8. T1566 PHISHING
9. T1530 DATA FROM CLOUD STORAGE
10. T1080 TAINT SHARED CONTENT

DOWNLOAD

T1078 VALID ACCOUNTS

DESCRIPTION

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop.(Citation: volexity_0day_sophos_FW) Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account. (Citation: CISA MFA PrintNightmare)

The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.(Citation: TechNet Credential Theft)

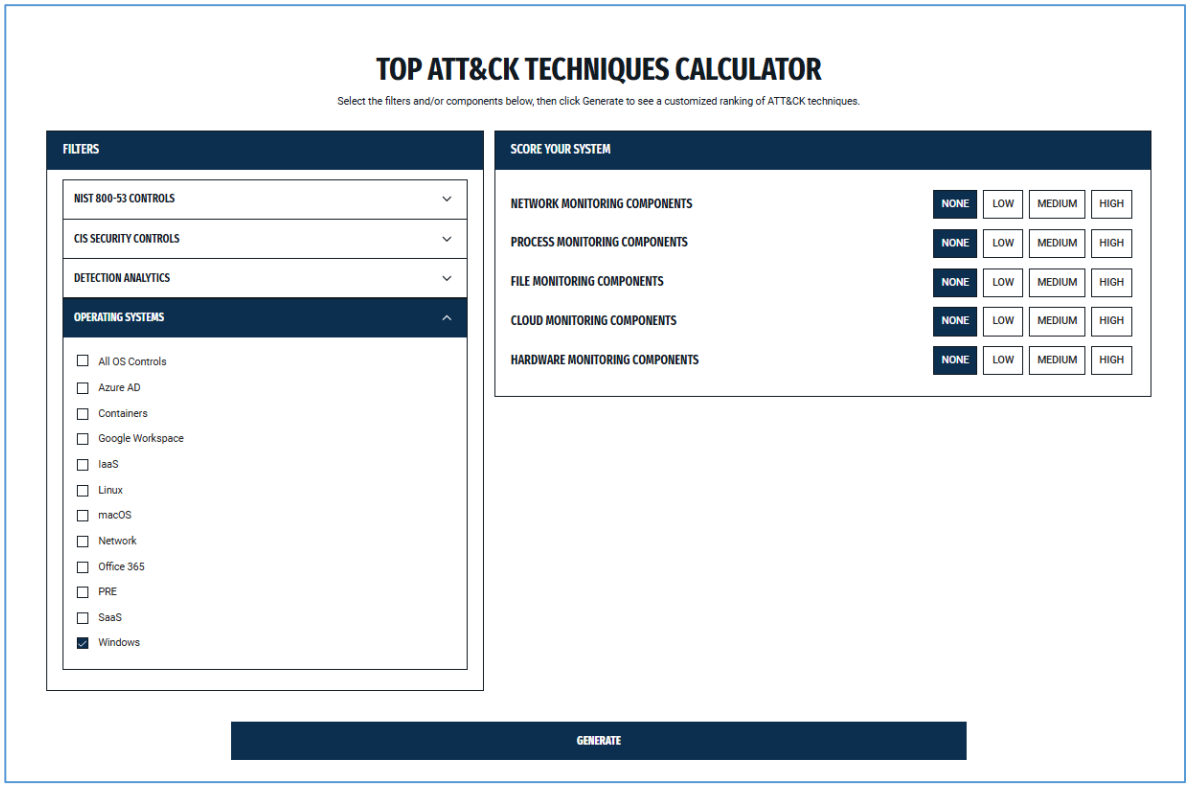
SUBTECHNIQUES

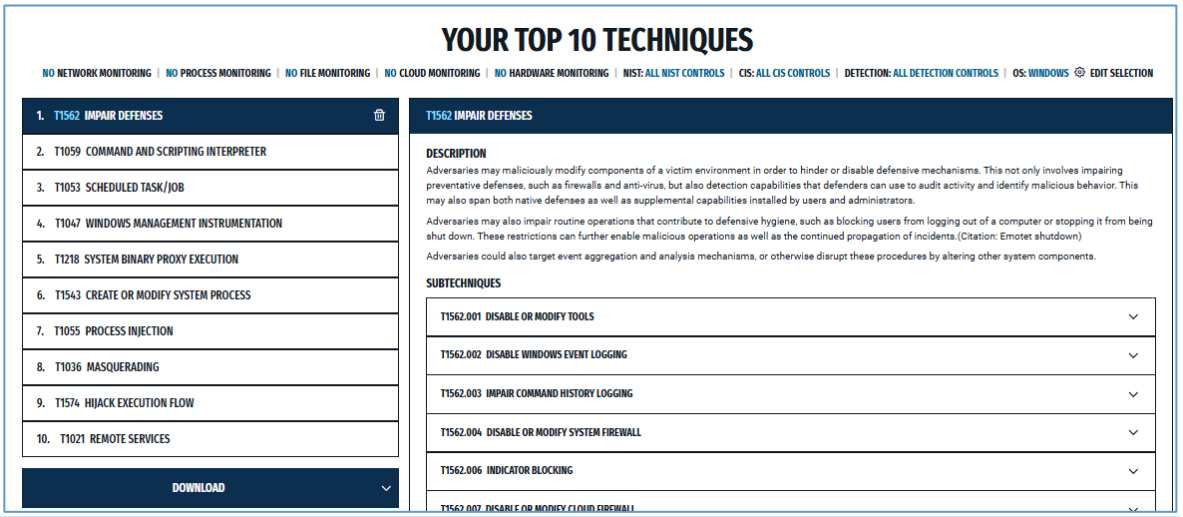
- T1078.001 DEFAULT ACCOUNTS
- T1078.002 DOMAIN ACCOUNTS
- T1078.003 LOCAL ACCOUNTS

SaaS.json 9+, U

esktop > GeekBrains-specialization-ELECTIVES > 13. Fundamentals of Information Security > Seminar-02 > TopTenTechniques > {} SaaS.json > ...


```
"rank": 1,
"tid": "T1078",
"name": "Valid Accounts",
"description": "Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privil
"url": "https://attack.mitre.org/techniques/T1078",
"detection": "Configure robust, consistent account activity audit policies across the enterprise and with externally accessible services.(C
"score": 1.629267142857142,
"mitigations": [
    {
        "mid": "M1036",
        "name": "Account Use Policies",
        "description": "Configure features related to account use like login attempt lockouts, specific login times, etc.",
        "url": "https://attack.mitre.org/mitigations/M1036"
    },
    {
        "mid": "M1015",
        "name": "Active Directory Configuration",
        "description": "Configure Active Directory to prevent use of certain techniques; use SID Filtering, etc.",
        "url": "https://attack.mitre.org/mitigations/M1015"
    },
    {
        "mid": "M1013",
        "name": "Application Developer Guidance",
        "description": "This mitigation describes any guidance or training given to developers of applications to avoid introducing securit
```



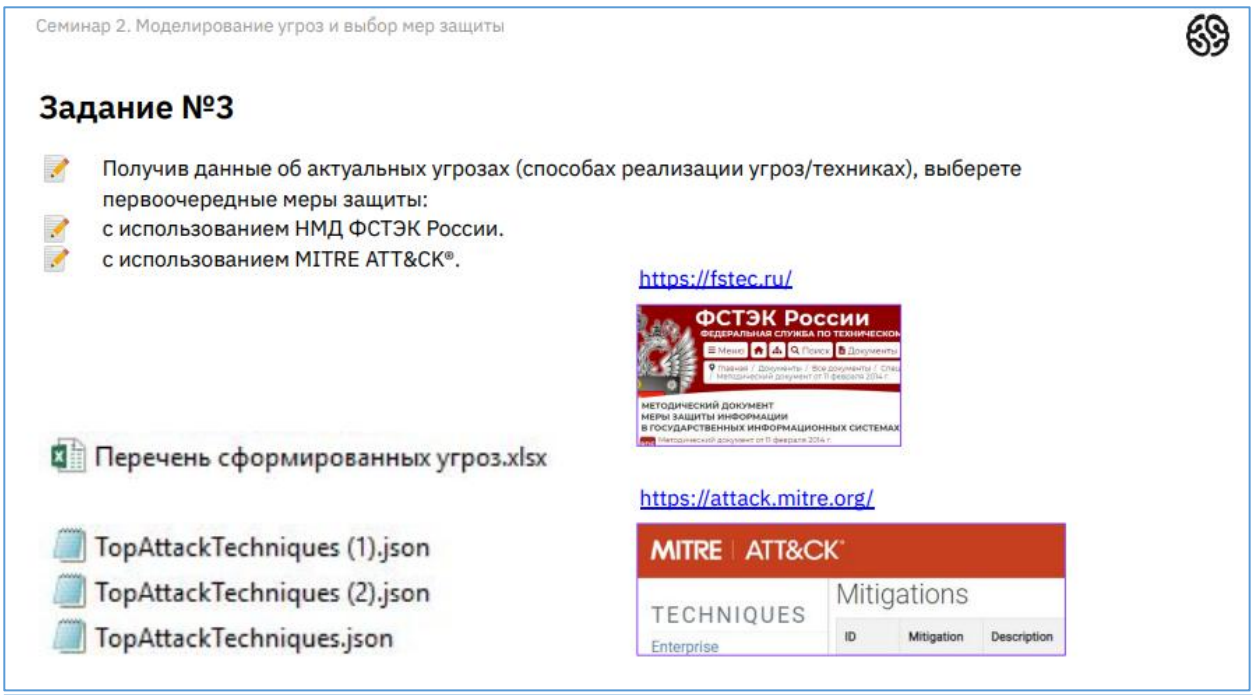


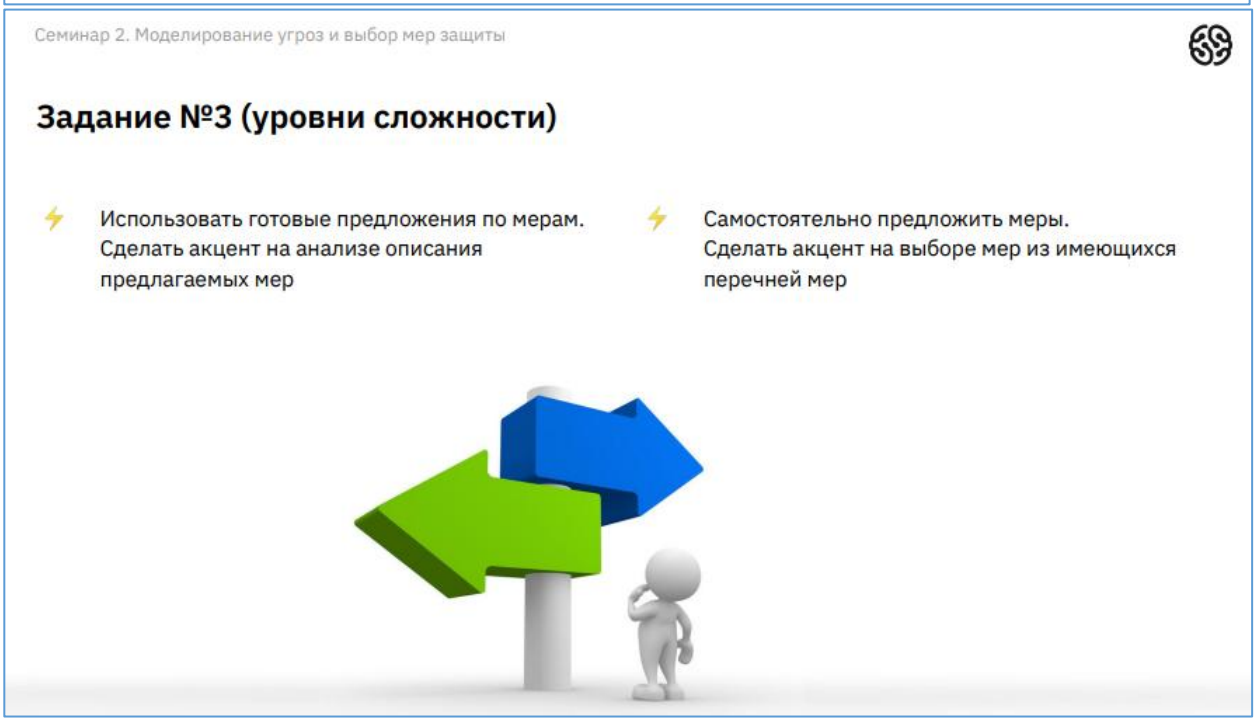
Windows.json 9+, U

C: > Users > user > Desktop > GeekBrains-specialization-ELECTIVES > 13. Fundamentals of Information Security > Seminar-02 > TopTenTechniques > {} Windows.json > ...


```
[
    {
        "rank": 1,
        "tid": "T1562",
        "name": "Impair Defenses",
        "description": "Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive me
        "url": "https://attack.mitre.org/techniques/T1562",
        "detection": "Monitor processes and command-line arguments to see if security tools or logging services are killed or stop runni
        "score": 3.6095241904761903,
        "mitigations": [
            {
                "mid": "M1047",
                "name": "Audit",
                "description": "Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to ide
                "url": "https://attack.mitre.org/mitigations/M1047"
            },
            {
                "mid": "M1038",
                "name": "Execution Prevention",
                "description": "Block execution of code on a system through application control, and/or script blocking.",
                "url": "https://attack.mitre.org/mitigations/M1038"
            },
            {
                "mid": "M1022",
                "name": "Restrict File and Directory Permissions",
                "description": "Restrict access by setting directory and file permissions that are not specific to users or privileged a
```

Задание 3


Семинар 2. Моделирование угроз и выбор мер защиты
Задание №3
Получив данные об актуальных угрозах (способах реализации угроз/техниках), выберете первоочередные меры защиты:
с использованием НМД ФСТЭК России.
с использованием MITRE ATT&CK®.
https://fstec.ru/
ФСТЭК России
ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМ
МЕТОДИЧЕСКИЙ ДОКУМЕНТ
МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ
В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ
Перечень сформированных угроз.xlsx
https://attack.mitre.org/
TopAttackTechniques (1).json
TopAttackTechniques (2).json
TopAttackTechniques.json
MITRE | ATT&CK
TECHNIQUES
Enterprise
Mitigations
ID
Mitigation
Description


Семинар 2. Моделирование угроз и выбор мер защиты
Задание №3 (уровни сложности)
Использовать готовые предложения по мерам. Сделать акцент на анализе описания предлагаемых мер
Самостоятельно предложить меры. Сделать акцент на выборе мер из имеющихся перечней мер

Искать ОЦЛ.1 Подсказка

Приказ ФСТЭК России от 25 декабря 2017 г. N 239

решающих правил + + VIII. Обеспечение целостности (ОЦЛ) ОЦЛ.0 Регламентация правил и процедур обеспечения целостности + + + ОЦЛ.1 Контрол целостности программного обеспечения + + + ОЦЛ.2 Контроль целостности информации ОЦЛ.3 Ограничения по вводу...

Приказ ФСТЭК России от 14 марта 2014 г. N 31

базы решающих правил + + VIII. Обеспечение целостности (ОЦЛ) ОЦЛ.0 Разработка политики обеспечения целостности + + + ОЦЛ.1 Контроль целостност программного обеспечения + + + ОЦЛ.2 Контроль целостности информации ОЦЛ.3 Ограничения по вводу информации в...

Приказ ФСТЭК России от 18 февраля 2013 г. N 21

пользователей в информационной системе + + IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ) ОЦЛ.1 Контрол целостности программного обеспечения, включая программное обеспечение средств защиты информации + + ОЦЛ.2 Контроль...

Приказ ФСТЭК России от 11 февраля 2013 г. N 17

пользователей в информационной системе + + + IX. Обеспечение целостности информационной системы и информации (ОЦЛ) ОЦЛ.1 Контроль целостност программного обеспечения, включая программное обеспечение средств защиты информации + + ОЦЛ.2 Контроль...

Показано **1** - **4** из **4**

ТРЕБОВАНИЯ
ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

I. Общие положения

1. Настоящие Требования разработаны в соответствии с Федеральным законом от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" и направлены на обеспечение устойчивого функционирования значимых объектов критической информационной инфраструктуры Российской Федерации (далее – значимые объекты, критическая информационная инфраструктура) при проведении в отношении них компьютерных атак.

2. Действие настоящих Требований распространяется на информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети, которые отнесены к значимым объектам критической информационной инфраструктуры в соответствии со статьей 7 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

3. По решению субъекта критической информационной инфраструктуры настоящие Требования могут применяться для обеспечения безопасности объектов критической информационной инфраструктуры, не отнесенных к значимым объектам.

4. Обеспечение безопасности значимых объектов, в которых обрабатывается информация, составляющая государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

5. Для обеспечения безопасности значимых объектов, являющихся информационными системами персональных данных, настоящие Требования применяются с учетом Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 (Собрание законодательства Российской Федерации, 2012, N 45, ст. 6257).

Для обеспечения безопасности значимых объектов, являющихся государственными информационными системами, настоящие Требования применяются с учетом Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. N 17 (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный N 28608) (с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 г. N 27 "О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. N 17" (зарегистрирован Минюстом России 14 марта 2017 г., регистрационный N 45933).

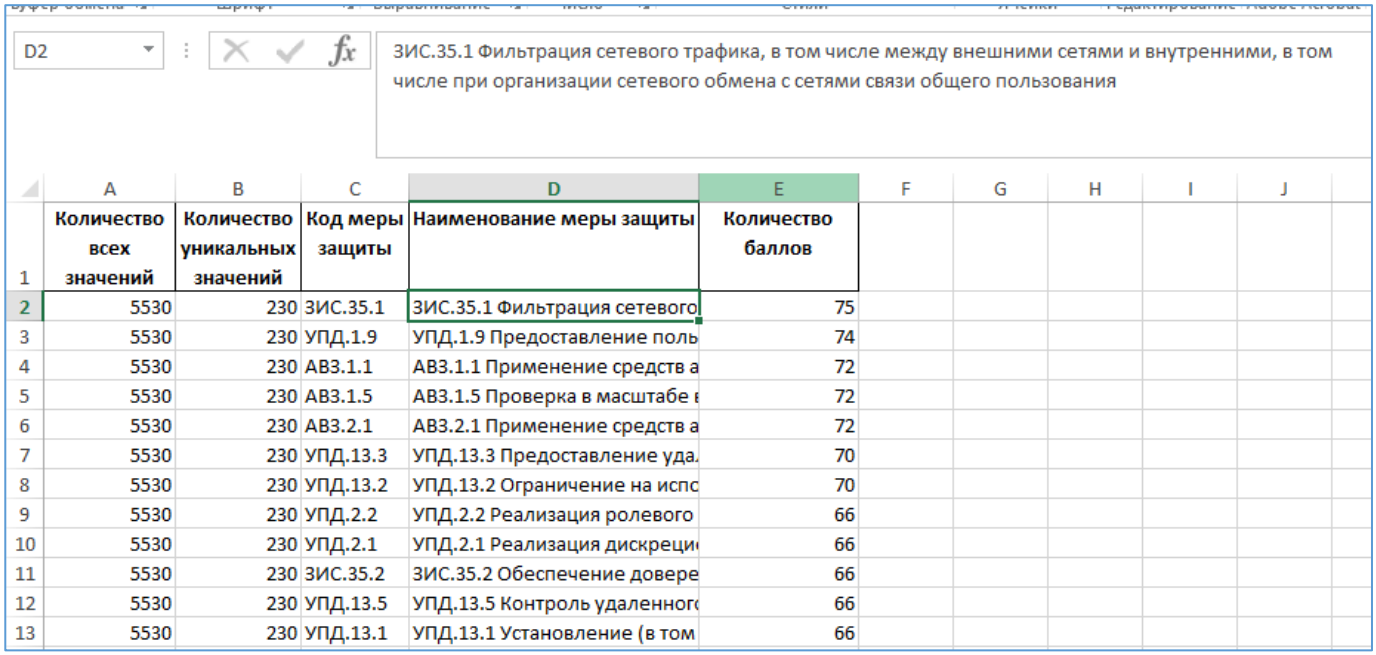
Домашняя работа

Используя полученный в ходе выполнения файл XLSX/CSV-файла «Перечень сформированных угроз», сформируйте перечень уникальных мер защиты, подсчитав вклад каждой меры в нейтрализацию соответствующего способа реализации угрозы (+1 балл). Отсортируйте полученный перечень по убыванию в части полученных баллов. Можно сделать с использованием Microsoft Excel, Google Sheets или написать обработчик CSV-файла на Python.

Доп. задание: сделайте маппинг полученных мер с мерами из CIS Controls и/или NIST Cybersecurity Framework (CSF) там, где это возможно.

Направьте ответ в табличном формате с использованием Google Docs:
— код меры защиты
— наименование меры защиты
— количество баллов
— наименование меры на английском языке из CIS Controls (опционально)
— наименование меры на английском языке из NIST CSF (опционально).

```
import pandas as pd

# Загрузить CSV-файл в DataFrame
df = pd.read_csv('Перечень сформированных угроз.csv')

# Столбец 'Меры защиты' содержит значения, разделенные ';'
# Разделить столбец и развернуть его
df['Меры защиты'] = df['Меры защиты'].str.split(';')
df = df.explode('Меры защиты')

# Посчитать количество всех значений
total_count = df['Меры защиты'].size

# Посчитать количество уникальных значений
unique_count = df['Меры защиты'].nunique()

# Посчитать количество каждого значения
value_counts = df['Меры защиты'].value_counts()

# Создание DataFrame с результатами
results = pd.DataFrame({
    'Количество всех значений': total_count,
    'Количество уникальных значений': unique_count,
    'Код меры защиты': [row.split(' ')[0] for row in value_counts.index],
    'Наименование меры защиты': value_counts.index,
    'Количество баллов': value_counts
})

# Сортировка по убыванию количества баллов
results = results.sort_values(by='Количество баллов', ascending=False)

# Сохранение в Excel файл
output_file = 'Отсортированный перечень сформированных угроз.xlsx'
results.to_excel(output_file, index=False)
```



D2

ЗИС.35.1 Фильтрация сетевого трафика, в том числе между внешними сетями и внутренними, в том числе при организации сетевого обмена с сетями связи общего пользования

	A	B	C	D	E	F	G	H	I	J
1	Количество всех значений	Количество уникальных значений	Код меры защиты	Наименование меры защиты	Количество баллов					
2	5530	230	ЗИС.35.1	ЗИС.35.1 Фильтрация сетевого	75					
3	5530	230	УПД.1.9	УПД.1.9 Предоставление поль	74					
4	5530	230	АВЗ.1.1	АВЗ.1.1 Применение средств а	72					
5	5530	230	АВЗ.1.5	АВЗ.1.5 Проверка в масштабе в	72					
6	5530	230	АВЗ.2.1	АВЗ.2.1 Применение средств а	72					
7	5530	230	УПД.13.3	УПД.13.3 Предоставление уда	70					
8	5530	230	УПД.13.2	УПД.13.2 Ограничение на испс	70					
9	5530	230	УПД.2.2	УПД.2.2 Реализация ролевого	66					
10	5530	230	УПД.2.1	УПД.2.1 Реализация дискреци	66					
11	5530	230	ЗИС.35.2	ЗИС.35.2 Обеспечение довере	66					
12	5530	230	УПД.13.5	УПД.13.5 Контроль удаленного	66					
13	5530	230	УПД.13.1	УПД.13.1 Установление (в том	66					

Ссылка на репозиторий:
https://github.com/olgashenkel/GeekBrains-specialization-ELECTIVES/tree/main/13.%20Fundamentals%20of%20Information%20Security