УДК 004.056.5

Грибалев Л.А., Мутовин Д.С.

РГУ нефти и газа (НИУ) имени И.М. Губкина, Москва, Россия

Кафедра безопасности информационных технологий

АНАЛИЗ УЯЗВИМОСТИ CVE-2025-20362 В КОМПОНЕНТЕ WEBVPN CISCO ASA: ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ОБХОДА АВТОРИЗАЦИИ

Аннотация. *В статье представлено экспериментальное исследование уязвимости CVE-2025-20362 в компоненте WebVPN межсетевых экранов Cisco ASA и FTD. Уязвимость относится к классу Missing Authorization (CWE-862) и эксплуатирует некорректную нормализацию URL-путей, что соответствует технике T1190 (Exploit Public-Facing Application) матрицы MITRE ATT&CK. В работе явно сформулирована научная гипотеза об обходе механизма авторизации посредством path traversal последовательности, экспериментально проверена на реальном оборудовании Cisco ASA 5506-X (версия 9.8(2)) и подтверждена методом контрольного сравнения. Проведена количественная оценка риска по методике ФСТЭК России. Рассмотрены ограничения исследования и намечены направления дальнейшей работы.*

Ключевые слова: *CVE-2025-20362, Cisco ASA, WebVPN, path traversal, Missing Authorization, CWE-862, MITRE ATT&CK T1190, обход аутентификации, оценка рисков ФСТЭК, сетевая безопасность.*

Annotation. *The article presents an experimental study of the vulnerability CVE-2025-20362 in the WebVPN component of Cisco ASA and FTD firewalls. The vulnerability belongs to the Missing Authorization class (CODE-862) and exploits incorrect normalization of URL paths, which corresponds to the T1190 (Exploit Public-Facing Application) technique of the MITRE ATT&CK matrix. The paper explicitly formulates a scientific hypothesis about bypassing the authorization mechanism by means of a path traversal sequence, experimentally tested on real Cisco ASA 5506-X equipment (version 9.8(2)) and confirmed by a control*

comparison method. A quantitative risk assessment was carried out using the FSTEC methodology. The limitations of the study are considered and the directions of further work are outlined.

Keywords: *CVE-2025-20362, Cisco ASA, WebVPN, path traversal, Missing Authorization, CODE-862, MITRE ATT&CK T1190, authentication bypass, FSTEC risk assessment, network security.*

1. Введение

Межсетевые экраны серии Cisco ASA занимают одно из ключевых мест в инфраструктуре сетевой безопасности корпоративного уровня, в том числе на объектах топливно-энергетического комплекса. Задачи классификации и управления трафиком, характерные для таких объектов, рассматриваются в работах по анализу сетевой инфраструктуры [1]. Однако любые средства защиты могут содержать уязвимости, компрометирующие всю выстроенную систему защиты.

Уязвимости в аутентификационных механизмах широко рассматриваются в академической литературе. В работе [2] проведён анализ методов разграничения доступа в информационных системах и показано, что ошибки в логике авторизации являются одним из наиболее распространённых классов дефектов. В [3] авторы исследуют уязвимости веб-компонентов корпоративных систем и классифицируют атаки на обход авторизации, указывая на их устойчивое присутствие в OWASP Top 10 — в категории A01:2021 «Нарушение управления доступом». В матрице MITRE ATT&CK техника T1190 (Exploit Public-Facing Application) входит в тактику Initial Access и охватывает эксплуатацию уязвимостей публично доступных приложений, в том числе устройств сетевой инфраструктуры [4].

25 сентября 2025 года Cisco раскрыла уязвимость CVE-2025-20362 в WebVPN-компоненте межсетевых экранов ASA и FTD. Несмотря на оценку CVSS 6.5 (Medium), уязвимость была незамедлительно включена CISA в каталог Known Exploited Vulnerabilities [5], что свидетельствует об активной эксплуатации. Количественная оценка реальной опасности CVE требует выхода за рамки базовой метрики CVSS: как показано в [6], ранжирование уязвимостей только по технической критичности без учёта контекста развёртывания приводит к неверной расстановке приоритетов при управлении рисками. Вопросы комплексной методики обнаружения и оценки уязвимостей сетевой инфраструктуры рассмотрены в [7].

Path traversal как класс уязвимостей изучен в литературе преимущественно применительно к файловым системам и веб-приложениям [8]. Применение данной техники для обхода логического разграничения зон URL-пространства в устройствах сетевой безопасности является менее исследованным вектором, что обусловливает актуальность настоящей работы. Анализ рисков кибербезопасности АСУ ТП, в том числе с применением

методик ФСТЭК, рассматривается в [9], а моделирование угроз на объектах информатизации — в [10].

Цель работы — экспериментальное подтверждение гипотезы об обходе механизма авторизации WebVPN посредством path traversal последовательности на реальном оборудовании Cisco ASA, а также количественная оценка риска и разработка мер защиты.

Для достижения цели поставлены следующие **задачи:**

1. Анализ архитектуры URL-пространства компонента WebVPN Cisco ASA и механизма работы авторизационного модуля.
2. Формализация научной гипотезы об условиях обхода авторизации с определением нулевой и альтернативной гипотез и критерия их проверки.
3. Разработка методики сравнительного эксперимента на реальном оборудовании.
4. Проведение экспериментов и верификация гипотезы.
5. Количественная оценка риска эксплуатации по методике ФСТЭК России.
6. Разработка мер по устранению уязвимости и обнаружению атак.
7. Определение ограничений исследования и направлений дальнейшей работы.

2. Гипотеза исследования

Анализ структуры URL-пространства WebVPN и описания механизма уязвимости CVE-2025-20362 позволяет сформулировать следующую научную гипотезу:

> *Последовательность /../ в контексте запроса /+CSCOU+//../+CSCOE+/ позволяет обойти механизм разграничения публичной и защищённой зон URL-пространства веб-сервера Cisco ASA, поскольку авторизационная проверка выполняется на основании начального префикса пути без предварительной нормализации URI согласно RFC 3986 [11], что создаёт условие TOCTOU (Time of Check to Time of Use) и даёт неаутентифицированному пользователю доступ к ресурсам зоны /+CSCOE+/.*

Формальная постановка:

– H_0 (нулевая): Механизм авторизации ASA нормализует URI до выполнения проверки прав доступа; обход посредством path traversal невозможен.

– H_1 (альтернативная): Нормализация URI выполняется после авторизационной проверки; traversal-последовательность позволяет обойти разграничение зон.

Критерий принятия H_1: получение ответа HTTP 200 OK с обработкой запроса в контексте зоны /+CSCOE+/ без перенаправления на страницу аутентификации при использовании traversal-URL. Критерий принятия H_0: перенаправление на страницу входа (аналогично контрольному запросу).

3. Техническое описание уязвимости

3.1 Архитектура URL-пространства WebVPN

Веб-сервер компонента WebVPN организует URL-пространство на основе двух логических зон:

– /+CSCOU+/ — публичная зона (unauthenticated): статические ресурсы страниц входа, CSS, JavaScript, доступные без аутентификации;

– /+CSCOE+/ — защищённая зона (authenticated): функциональные эндпоинты WebVPN (управление файлами, порталы, настройки сессий), требующие успешной аутентификации.

Разграничение реализовано через авторизационный модуль веб-сервера, анализирующий входящий URL для определения зоны принадлежности ресурса. Класс таких ошибок — Missing Authorization (CWE-862) — характеризуется отсутствием или некорректностью проверки прав доступа перед выполнением действия [12].

3.2 Механизм уязвимости (TOCTOU в нормализации URI)

Уязвимость CVE-2025-20362 обусловлена нарушением принципа «нормализация до проверки»: авторизационный модуль анализирует начальный компонент пути без предварительного приведения URI к каноническому виду. При получении запроса /+CSCOU+//../+CSCOE+/endpoint последовательность обработки выглядит следующим образом:

1. Авторизационная проверка: сервер обнаруживает префикс /+CSCOU+/ → `запрос классифицирован как публичный` → `аутентификация не требуется.`
2. Передача URI в модуль маршрутизации запросов.
3. `Нормализация URI: /+CSCOU+//../ разрешается как переход в родительский каталог → итоговый путь /+CSCOE+/endpoint.`
4. Обработка запроса в контексте защищённой зоны без проверки аутентификации.

Расхождение между моментом проверки (шаг 1) и моментом использования URI (шаг 4) представляет собой структурный дефект типа TOCTOU. Аналогичная природа ошибки описана в [13] применительно к уязвимостям обхода директорий в веб-серверах.

3.3 Классификация и оценка

Параметр	Значение
Идентификатор CVE	CVE-2025-20362
Класс (CWE)	CWE-862: Missing Authorization
CVSS v3.1 Base Score	6.5 Medium; AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
MITRE ATT&CK	T1190 — Exploit Public-Facing Application (Initial Access)
Дата раскрытия	25 сентября 2025 г. (cisco-sa-asaftd-webvpn-YROOTUW)
Статус CISA KEV	Включена (активная эксплуатация подтверждена)
Условие эксплуатации	WebVPN включён на внешнем интерфейсе, порт 443 доступен

Таблица 1 — Классификационные параметры CVE-2025-20362

3.4 Затронутые версии

Продукт	Уязвимые версии	Исправленная версия
Cisco ASA	9.8.x – 9.16.x до 9.16.4.84	9.16.4.85
Cisco ASA	9.18.x до 9.18.4.66	9.18.4.67
Cisco ASA	9.20.x до 9.20.4.9	9.20.4.10
Cisco ASA	9.22.x до 9.22.2.13	9.22.2.14
Cisco FTD	7.0.x до 7.0.8.0	7.0.8.1
Cisco FTD	7.2.x до 7.2.10.1	7.2.10.2

Таблица 2 — Затронутые версии Cisco ASA и Cisco FTD [14]

4. Методология эксперимента

4.1 Лабораторный стенд

Принципиальной особенностью данного исследования является проведение экспериментов на реальном оборудовании, а не на виртуальных машинах или эмуляторах. Состав стенда представлен в таблице 3.

Компонент	Характеристики	Роль
Cisco ASA 5506-X	Прошивка ASA 9.8(2), версия входит в диапазон уязвимых	Целевое устройство (объект исследования)

ПК1 (исследователь)	ALT Education 10.2, IP: 10.19.103.50	Формирование и отправка HTTP-запросов
Консольный сервер	IP: 10.19.103.27, порт 7010 (Telnet)	Управление конфигурацией ASA

Таблица 3 — Состав лабораторного стенда

Все устройства подключены к подсети 10.19.103.0/24, что моделирует сегмент периметральной защиты. Выбор версии 9.8(2) обусловлен её принадлежностью к диапазону уязвимых прошивок ASA 9.8.x.

4.2 Конфигурация целевого устройства

На Cisco ASA 5506-X выполнена минимально необходимая конфигурация, воспроизводящая условия эксплуатации уязвимости. Настройка внешнего интерфейса:

```
ciscoasa# configure terminal
ciscoasa(config)# interface
GigabitEthernet1/1 ciscoasa(config-if)# nameif
outside ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.19.103.100 255.255.255.0
ciscoasa(config-if)# no shutdown
```

Активация WebVPN на внешнем интерфейсе:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# enable outside
ciscoasa(config-webvpn)# anyconnect enable
ciscoasa(config-webvpn)# end
```

4.3 Метод контрольного сравнения

Применяемая методика основана на принципе единственного изменяемого фактора: два запроса к одному и тому же функциональному эндпоинту различаются только структурой URL. Это позволяет изолировать влияние traversal-последовательности как независимой переменной и исключить альтернативные интерпретации результатов. Для передачи traversal-последовательности без клиентской нормализации применяется флаг --path-as-is утилиты curl 8.12.0.

5. Проведение экспериментов и результаты

5.1 Эксперимент 1 — Контрольный запрос

Прямой запрос к защищённому эндпоинту /+CSCOE+/ без traversal-последовательности, моделирующий поведение неаутентифицированного клиента:

```
curl -k -v \

"https://10.19.103.100/+CSCOE+/files/file_action.html?mode=uploa
d " \
    -X POST -d "test"
```

Ответ сервера:

```
< HTTP/1.1 200 OK
< Set-Cookie: webvpn=;     expires=Thu, 01 Jan 1970 22:00:00
GMT; path=/; secure
< Set-Cookie: webvpnlogin=1; path=/; secure


  <html><script>
  document.location.replace("/+CSCOE+/logon.html");
</script></html>
```

Интерпретация: сервер идентифицировал запрос к защищённому ресурсу и инициировал процедуру аутентификации — все сессионные cookie аннулированы, выдано перенаправление на страницу входа. Поведение корректное, соответствует H_0.

5.2 Эксперимент 2 — Запрос с path traversal (проверка H_1)

Запрос с traversal-последовательностью: начало в публичной зоне /+CSCOU+/, переход в защищённую /+CSCOE+/ через /../:

```
curl -k -v --path-as-is \

"https://10.19.103.100/+CSCOU+//../+CSCOE+/files/file_action.html
\
    ?mode=upload&path=foo&server=srv&sourceurl=quz" \
    -X POST -d "aabbccdd"
```

Ответ сервера:

```
< HTTP/1.1 200 OK
< Content-Type: text/html; charset=utf-8


  <html><body><script>
  alert("Failed to upload file");
    location.href="/+CSCOE+/files/browse.html?code=init&path=quz"
</script></body></html>
```

Интерпретация: сервер обработал запрос в защищённом контексте без инициирования аутентификации. Сообщение «Failed to upload file» подтверждает, что запрос достиг логики файловой операции — авторизационный барьер преодолён. Перенаправление в теле ответа указывает на контекст зоны /+CSCOE+/ при отсутствии каких-либо аутентификационных проверок. H_1 принята.

6. Анализ и обсуждение результатов

6.1 Сравнительный анализ экспериментов

Параметр	Эксперимент 1 (контрольный)	Эксперимент 2 (CVE-2025-20362)
URL запроса	/+CSCOE+/files/...	/+CSCOU+//../+CSCOE+/files/...
Флаг --path-as-is	Не используется	Обязателен
HTTP-ответ	200 + редирект logon.html	200 + обработка операции
Авторизация	Инициирована (cookie сброшены)	Не проверялась
Контекст обработки	Публичный (/+CSCOU+/)	Защищённый (/+CSCOE+/)
Гипотеза	Поведение корректное (H_0)	Уязвимость подтверждена (H_1)

Таблица 4 — Сравнительный анализ результатов экспериментов

6.2 Количественная оценка риска по методике ФСТЭК

В соответствии с «Методикой оценки угроз безопасности информации» ФСТЭК России (2021) интегральный показатель риска определяется как произведение вероятности реализации угрозы и возможного ущерба [15].

Авторы работы [9] демонстрируют применение аналогичного подхода для АСУ ТП промышленных объектов.

Оценка составляющих риска CVE-2025-20362:

Параметр	Значение	Обоснование
Вероятность реализации угрозы (P)	Высокая (0,8)	Включена в KEV CISA; PoC-код опубликован; эксплуатация зафиксирована
Уровень ущерба — конфиденциальность (C)	Средний (0,5)	Доступ к закрытым эндпоинтам WebVPN без учётных данных
Уровень ущерба — целостность (I)	Средний (0,5)	Возможность файловых операций в защищённом контексте
Уровень ущерба — доступность (A)	Высокий (0,8)	Цепочка с CVE-2025-20333 приводит к DoS/перезагрузке устройства
Интегральный показатель риска R	0,52	$R = P \times \max(C, I, A) = 0,8 \times 0,65 \approx 0,52$ (критический уровень)

Таблица 5 — Количественная оценка риска по методике ФСТЭК

Полученное значение R = 0,52 соответствует критическому уровню риска по шкале ФСТЭК (пороговое значение критического уровня: R ≥ 0,5). Таким образом, несмотря на оценку CVSS 6.5 (Medium), реальная опасность CVE-2025-20362 значительно выше с учётом контекста развёртывания. Это согласуется с выводами [6] о недостаточности базовой CVSS-метрики для приоритизации уязвимостей.

6.3 Потенциальные последствия эксплуатации

В терминах MITRE ATT&CK [4] CVE-2025-20362 обеспечивает технику T1190 (Initial Access). В условиях реальной атаки это открывает следующие векторы:

– Несанкционированный доступ к защищённым эндпоинтам WebVPN без учётных данных.

– Построение цепочки атаки с CVE-2025-20333 (переполнение буфера в WebVPN): CVE-2025-20362 открывает доступ к уязвимому эндпоинту, CVE-2025-20333 обеспечивает RCE с привилегиями root [14].

– Отказ в обслуживании: по данным Cisco от ноября 2025 года, новый вариант атаки вызывает принудительную перезагрузку устройства [5].

– Разведка инфраструктуры: имена пользователей, группы политик, структура VPN-портала для последующих атак.

По данным открытых источников, на момент раскрытия уязвимости около 50 000 устройств Cisco ASA и FTD были доступны из Интернет [5], что подчёркивает масштаб потенциальных последствий.

7. Меры по устранению и обнаружению

7.1 Установка патча

Единственной надёжной мерой является обновление прошивки ASA до версии с исправлением (таблица 2). Для ветки 9.8.x, использованной в исследовании, рекомендуется переход на актуальную поддерживаемую ветку.

7.2 Временные меры при невозможности обновления

1. Отключение WebVPN на внешнем интерфейсе, если функция не используется:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# no enable outside
```

2. Ограничение доступа к порту 443 на уровне ACL или вышестоящего МСЭ до доверенных IP-адресов.

3. Усиленный мониторинг журналов с интеграцией в SIEM.

7.3 Обнаружение атаки

Признаки эксплуатации CVE-2025-20362 в журналах Cisco ASA:

– HTTP-запросы, содержащие паттерн +CSCOU+//../+CSCOE+/ в URI.
– Обращения к /+CSCOE+/ без предшествующей сессии аутентификации от данного IP.
– Аномально высокая частота запросов к защищённым эндпоинтам.

Команда диагностики:

```
ciscoasa# show logging | include CSCOE
```

Для IDS/IPS рекомендуется сигнатура с паттерном CSCOU.*\.\./.*CSCOE в URI HTTPS-запросов. Методология обнаружения вторжений в корпоративных системах, включая анализ аномалий на уровне веб-сервера, описана в [16].

8. Ограничения исследования

Настоящее исследование имеет следующие ограничения, которые необходимо учитывать при интерпретации результатов:

1. Тестирование на единственной модели и версии прошивки. Эксперименты проведены только на Cisco ASA 5506-X версии 9.8(2). Для повышения внешней валидности результатов необходима верификация на 2–3 дополнительных версиях из диапазона уязвимых (например, 9.18.x и 9.20.x). Результаты напрямую применимы к перечисленным в таблице 2 версиям, но детали поведения могут незначительно различаться.
2. Отсутствие оценки производительности. В ходе экспериментов не измерялось влияние traversal-запросов на загрузку CPU и память ASA. При массовой эксплуатации возможны вторичные эффекты на производительность, что требует отдельного исследования.

3. Ограничения лабораторной топологии. Стенд представляет собой плоскую сеть с одной подсетью без промежуточных прокси-серверов, IPS или WAF. В реальных корпоративных сетях наличие таких компонентов может модифицировать или блокировать traversal-запросы.
4. Неполное исследование цепочки атаки. Данная работа фокусируется исключительно на CVE-2025-20362 (обход авторизации). Демонстрация полной цепочки RCE совместно с CVE-2025-20333 выходит за рамки настоящего исследования.
5. Статичная конфигурация. Тестировалась только базовая конфигурация WebVPN без дополнительных мер защиты. Влияние нестандартных настроек (например, кастомных правил ACL или интеграции с AAA-серверами) на воспроизводимость уязвимости не исследовалось.

9. Заключение

В настоящей работе проведено экспериментальное исследование уязвимости CVE-2025-20362 в компоненте WebVPN межсетевых экранов Cisco ASA. Сформулирована и экспериментально проверена научная гипотеза об обходе механизма авторизации посредством path traversal последовательности. Нулевая гипотеза H_0 отклонена; принята альтернативная H_1.

Исследование выполнено на реальном оборудовании методом контрольного сравнения, что обеспечивает высокую внутреннюю валидность результатов. Количественная оценка риска по методике ФСТЭК показала критический уровень ($R = 0{,}52$), несмотря на умеренную базовую оценку CVSS 6.5, что подтверждает необходимость контекстной переоценки уязвимостей.

Уязвимость демонстрирует, что ошибки в последовательности «проверка–использование» (TOCTOU) применительно к нормализации URI способны полностью нивелировать механизмы авторизации в зрелых сетевых решениях. Корректная нормализация URI до выполнения авторизационной проверки является необходимым условием безопасной реализации любых механизмов разграничения доступа на основе URL-пространства.

Перспективными направлениями дальнейших исследований являются: верификация гипотезы на дополнительных версиях прошивок ASA; экспериментальная демонстрация полной цепочки атаки с CVE-2025-20333; разработка YARA/Sigma-правил для автоматизированного обнаружения эксплуатации.

Список использованных источников

1. Уймин, А. Г. Классификация корпоративного трафика с использованием алгоритмов машинного обучения / А. Г. Уймин // Автоматизация и информатизация ТЭК. – 2023. – № 7(600). – С. 22–29. – DOI 10.33285/2782-604X-2023-7(600)-22-29. – EDN WXXUPK.
2. Лифанова, О. В. Методы и средства аутентификации и авторизации пользователей в информационных системах / О. В. Лифанова // Вестник науки. – 2024. – № 5. – С. 44–51. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/metody-i-sredstva-autentifikatsii-i-avtorizatsii-polzovateley-v-informatsionnyh-sistemah
3. Галицкий, А. В. Классификация угроз и уязвимостей информационной безопасности в корпоративных системах / А. В. Галицкий, С. Д. Рябко // Вопросы кибербезопасности. – 2022. – № 3(49). – С. 18–27. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/klassifikatsiya-ugroz-i-uyazvimostey-informatsionnoy-bezopasnosti-v-korporativnyh-sistemah
4. MITRE Corporation. MITRE ATT&CK® Enterprise Matrix. Technique T1190:

Exploit Public-Facing Application [Электронный ресурс]. – 2024. – Режим доступа: https://attack.mitre.org/techniques/T1190/

5. CISA. Known Exploited Vulnerabilities Catalog – CVE-2025-20362. Emergency Directive ED 25-03 [Электронный ресурс]. – 2025. – Режим доступа: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

6. Малофеев, А. В. Комплексная методика обнаружения и оценкиуязвимостей информационной безопасности в сетевой инфраструктуре / А. В. Малофеев, П. С. Иванов // Вопросы кибербезопасности. – 2024. – № 4. – С. 35–46. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/kompleksnaya-metodika-obnaruzheniya-i-otsenki-uyazvimostey-informatsionnoy-bezopasnosti-v-setevoy-infrastrukture

7. Васильев, В. И. Методика оценки актуальных угроз и уязвимостей на основе технологий когнитивного моделирования и Text Mining / В. И. Васильев, А. М. Вульфин, Н. В. Кучкарова // Вопросы кибербезопасности. – 2022. – № 3. – С. 28–39. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/metodika-otsenki-aktualnyh-ugroz-i-uyazvimostey-na-osnove-tehnologiy-kognitivnogo-modelirovaniya-i-text-mining

8. Храпко, Р. Р. File Inclusion и Path Traversal как базовые уязвимости веб-приложений / Р. Р. Храпко // Хакер. – 2025. – Февраль. [Электронный ресурс]. – Режим доступа: https://xakep.ru/2025/02/07/file-inclusion-path-traversal/

9. Герасимов, А. В. Анализ рисков кибербезопасности АСУ ТП с помощью нечётких когнитивных карт / А. В. Герасимов, С. С. Куликов // Автоматизация в промышленности. – 2023. – № 2. – С. 14–22. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/analiz-riskov-kiberbezopasnosti-s-pomoschyu-nechetkih-kognitivnyh-kart

10. Моделирование угроз безопасности для построения КСЗИ на объектах информатизации

/ А. С. Марков [и др.] // Безопасность информационных технологий. –

2024. – Т. 31,

№ 1. – С. 41–53. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/modelirovanie-ugroz-bezopasnosti-dlya-postroeniya-kompleksnoy-sistemy-zaschity-informatsii-na-obektah-informatizatsii

11. Berners-Lee, T. Uniform Resource Identifier (URI): Generic Syntax / T. Berners-Lee, R. Fielding, L. Masinter // RFC 3986 [Электронный ресурс] / IETF. – 2005. – Режим доступа: https://www.rfc-editor.org/rfc/rfc3986

12. MITRE Corporation. CWE-862: Missing Authorization [Электронный ресурс]. – 2024. – Режим доступа: https://cwe.mitre.org/data/definitions/862.html

13. Исследование базовых атак и компрометации доменной Windows-инфраструктуры / Д. А. Морозов [и др.] // Прикаспийский журнал: управление и высокие технологии. – 2023. – № 4(64). – С. 81–93. [Электронный ресурс]. – Режим доступа:

https://cyberleninka.ru/article/n/issledovanie-bazovyh-atak-i-kompromentatsii-domennoy-windows-infrastruktury

14. Cisco Systems. Cisco Secure Firewall ASA and FTD Software WebVPN Unauthorized Access Vulnerability (cisco-sa-asaftd-webvpn-YROOTUW) [Электронный ресурс]. – 2025. – Режим доступа: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-YROOTUW
15. ФСТЭК России. Методика оценки угроз безопасности информации [Электронный ресурс]. – М., 2021. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskie-dokumenty
16. Темников, В. А. Модели и реализация обнаружения вторжений в корпоративной информационной системе с использованием интеллектуального подхода / В. А. Темников, Р. И. Ходжаев // Вестник СибГУ. – 2023. – № 2. – С. 105–113. [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/modeli-i-realizatsiya-obnaruzheniya-vtorzheniy-v-korporativnoy-informatsionnoy-sisteme-predpriyatiya-s-ispolzovaniem
17. Zscaler ThreatLabz. Cisco Firewall and VPN Zero-Day Attacks – CVE-2025-20333 and CVE-2025-20362 [Электронный ресурс]. – 2025. – Режим доступа: https://www.zscaler.com/blogs/security-research/cisco-firewall-and-vpn-zero-day- attacks-cve-2025-20333-and-cve-2025-20362
18. Horizon3.ai. CVE-2025-20362 / CVE-2025-20333 / CVE-2025-20363 Analysis [Электронный ресурс]. – 2025. – Режим доступа: https://horizon3.ai/attack-research/vulnerabilities/cve-2025-20362-cve-2025-20333-cve-2025-20363/