МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования «Санкт-Петербургский политехнический
университет Петра Великого»

Институт компьютерных наук и кибербезопасности

Высшая школа технологий искусственного интеллекта

Направление: 02.03.01 «Математика и компьютерные науки»

Отчёт по практическим работам по дисциплине «Защита информации»

Студент,
группы 5130201/20101 _____ Тищенко А. А.

Руководитель

_____ Силиненко А. В.

«____»_____ 2026г.

Санкт-Петербург, 2026

Содержание

Введение

В рамках курса «Защита информации» было выполнено несколько практических работ, по результатам которых был составлен данный отчёт, содержащий информацию по всем практическим работам. Отчетная информация по каждой работе – это отдельный раздел в общем отчете.

В отчёте представлены результаты следующих практических работ:

1. Практическая работа №1. Анализ уязвимостей программного обеспечения. Данная практическая работа посвящена анализу уязвимостей программного обеспечения с использованием Банка данных угроз безопасности информации ФСТЭК России [1]. В ходе выполнения работы предусмотрено изучение структуры разделов «Угрозы» и «Уязвимости», а также поиск уязвимостей по заданным критериям. Особое внимание уделяется выявлению уязвимостей, соответствующих используемым версиям операционных систем личных устройств, и рассмотрению возможных мер по их устранению.

1 Практическая работа №1. Анализ уязвимостей программного обеспечения

1.1 Знакомство с разделом «Угрозы» Банка угроз

Раздел «Угрозы» Банка данных угроз безопасности информации ФСТЭК России предназначен для систематизированного представления сведений об актуальных угрозах безопасности информации. Данный раздел содержит структурированную информацию, позволяющую оценить характер угроз, возможные последствия их реализации и способы противодействия.

Раздел включает в себя следующие основные аспекты:

1. Классификация угроз: угрозы распределяются по различным категориям в зависимости от источника возникновения, способа реализации и объекта воздействия. Это позволяет упорядочить информацию и упростить её анализ.

2. Описание угроз: для каждой угрозы приводится развернутое описание, включающее возможные сценарии реализации, цели нарушителя и потенциальные последствия для информационной системы.

3. Объекты воздействия: указываются типы информационных систем, ресурсов или процессов, на которые может быть направлена угроза.

4. Уровень опасности: каждой угрозе присваивается определённый уровень опасности, отражающий степень потенциального ущерба при её реализации.

5. Рекомендации по противодействию: приводятся общие меры и подходы, направленные на предупреждение реализации угрозы или снижение возможных негативных последствий.

1.2 Знакомство с разделом «Уязвимости» Банка угроз

Раздел «Уязвимости» Банка данных угроз безопасности информации ФСТЭК России предназначен для получения сведений об актуальных уязвимостях программного обеспечения и их характеристиках. В рамках работы были рассмотрены подразделы: «Список уязвимостей», «Наиболее опасные уязвимости» и «Инфографика».

Список уязвимостей представляет собой структурированный перечень выявленных уязвимостей в программном обеспечении. Для каждой уязвимости указывается идентификатор, наименование, описание, затронутое программное обеспечение и его версии, уровень опасности, а также оценка по шкале CVSS. Уязвимости классифицируются по уровню критичности (критический, высокий, средний и др.), что позволяет определить приоритетность их устранения. Также приводятся рекомендации по устранению или минимизации последствий эксплуатации уязвимости.

Подраздел «Наиболее опасные уязвимости» содержит перечень уязвимостей с наивысшим уровнем опасности. Как правило, к ним относятся уязвимости, позволяющие выполнить удалённое выполнение кода, повысить привилегии, обойти механизмы аутентификации или получить несанкционированный доступ к информации. Данный раздел позволяет оперативно определить наиболее критичные риски для информационных систем.

BDU:2026-02102	Уязвимость функции addJS() библиотеки для создания PDF-файлов jsPDF, позволяющая нарушителю выполнить произвольный код	19.02.2026
BDU:2026-01979	Уязвимость прикладного программного интерфейса api.values.get микропрограммного обеспечения IP-телефонов Grandstream GXP, позволяющая нарушителю выполнить произвольный код с правами root	18.02.2026
BDU:2026-02014	Уязвимость компонента libvpx браузеров Mozilla Firefox, Firefox ESR и почтового клиента Thunderbird, позволяющая нарушителю вызвать отказ в обслуживании	16.02.2026
BDU:2026-02017	Уязвимость функции multi_ssid файла /cgi-bin/wireless.cgi микропрограммного обеспечения маршрутизаторов Wavlink WL-WN579A3, позволяющая нарушителю выполнить произвольные команды	15.02.2026
BDU:2026-02019	Уязвимость функции Delete_Mac_list файла /cgi-bin/wireless.cgi микропрограммного обеспечения маршрутизаторов Wavlink WL-WN579A3, позволяющая нарушителю выполнить произвольные команды	15.02.2026

Рис. 1. Пример отображения наиболее опасных уязвимостей

Подраздел «Инфографика» предназначен для наглядного представления статистических данных по уязвимостям. В нём отображается распределение уязвимостей по уровням опасности, типам ошибок, видам программного обеспечения и производителям. Инфографика позволяет визуально оценить текущее состояние защищённости программных продуктов и выявить наиболее проблемные направления.

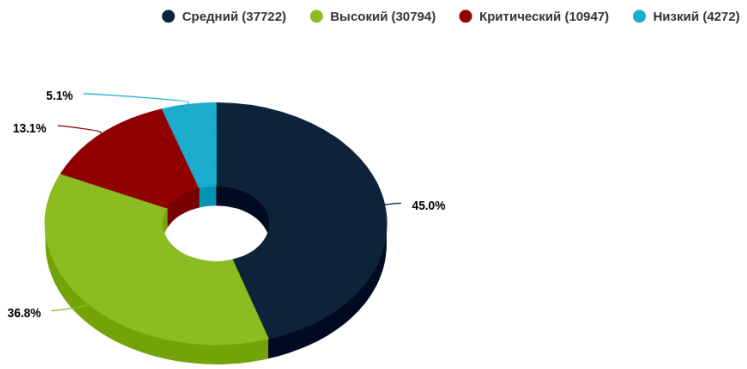


Рис. 2. Пример статистического распределения уязвимостей

1.3 Версии ОС, используемые в личных устройствах

На личном компьютере используется операционная система Ubuntu 25.10 (см. Рис. 3).

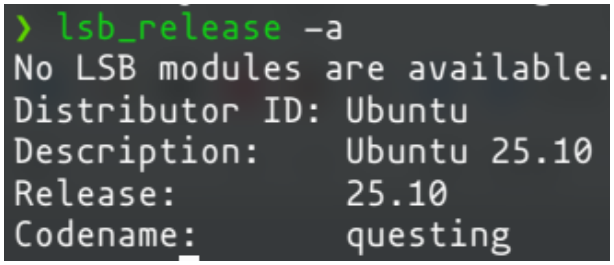


Рис. 3. Версия операционной системы личного компьютера

На личном мобильном устройстве используется операционная система Android 11 с графической оболочкой MIUI Global 12.5.14, сборка 12.5.14.0 RKURUXM (см. Рис. 4).

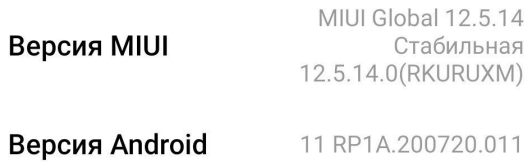


Рис. 4. Версия операционной системы личного мобильного устройства

1.4 Уязвимости ОС личного компьютера

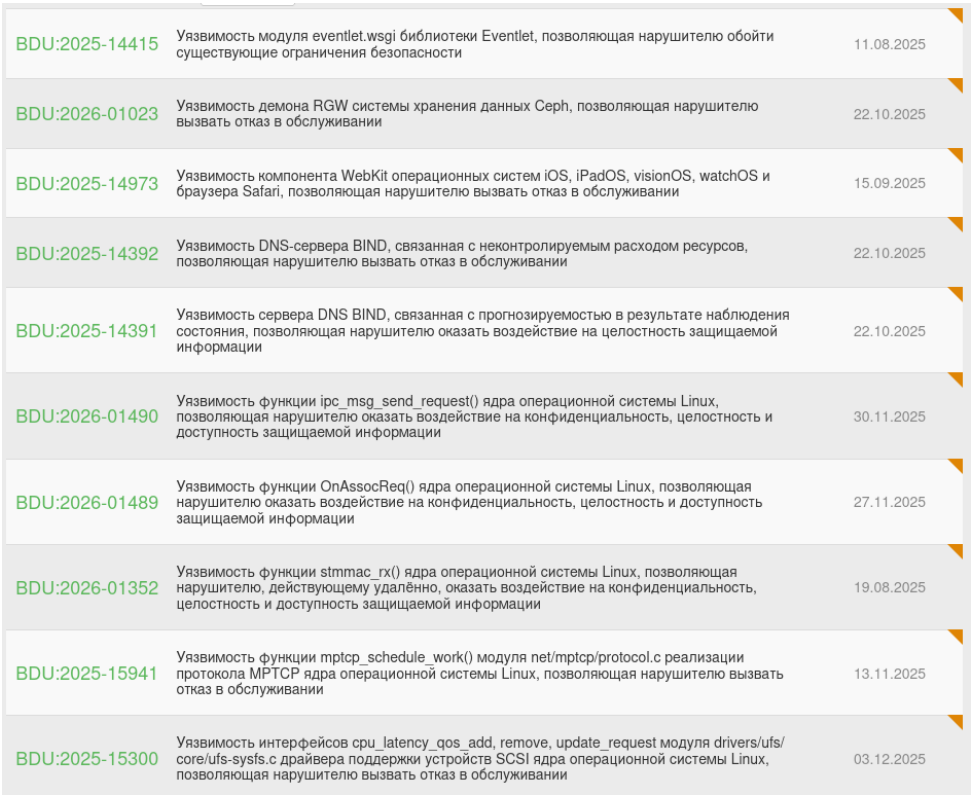
Для поиска уязвимостей ОС личного компьютера на сайте Банка данных угроз безопасности информации ФСТЭК России были использованы следующие критерии:

1. Операционная система: Ubuntu 25.10.
2. Уровень опасности: высокий.

Использовался уровень опасности «высокий», так как критических уязвимостей для данной ОС не найдено.

По заданным критериям было найдено 10 уязвимостей (см. Рис. 5).

Наиболее свежей является уязвимость BDU:2025-15300 «Уязвимость интерфейсов cpu_latency_qos_add, remove, update_request модуля drivers/ufs/core/ufs-sysfs.c драйвера поддержки устройств SCSI ядра операционной системы Linux связана с ошибками синхронизации при использовании общего ресурса («Ситуация гонки»). Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании». Развёрнутое описание уязвимости представлено на рисунке 6.



BDU:2025-14415	Уязвимость модуля eventlet.wsgi библиотеки Eventlet, позволяющая нарушителю обойти существующие ограничения безопасности	11.08.2025
BDU:2026-01023	Уязвимость демона RGW системы хранения данных Ceph, позволяющая нарушителю вызвать отказ в обслуживании	22.10.2025
BDU:2025-14973	Уязвимость компонента WebKit операционных систем iOS, iPadOS, visionOS, watchOS и браузера Safari, позволяющая нарушителю вызвать отказ в обслуживании	15.09.2025
BDU:2025-14392	Уязвимость DNS-сервера BIND, связанная с неконтролируемым расходом ресурсов, позволяющая нарушителю вызвать отказ в обслуживании	22.10.2025
BDU:2025-14391	Уязвимость сервера DNS BIND, связанная с прогнозируемостью в результате наблюдения состояния, позволяющая нарушителю оказать воздействие на целостность защищаемой информации	22.10.2025
BDU:2026-01490	Уязвимость функции ipc_msg_send_request() ядра операционной системы Linux, позволяющая нарушителю оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации	30.11.2025
BDU:2026-01489	Уязвимость функции OnAssocReq() ядра операционной системы Linux, позволяющая нарушителю оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации	27.11.2025
BDU:2026-01352	Уязвимость функции stmmac_rx() ядра операционной системы Linux, позволяющая нарушителю, действующему удалённо, оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации	19.08.2025
BDU:2025-15941	Уязвимость функции mptcp_schedule_work() модуля net/mptcp/protocol.c реализации протокола MPTCP ядра операционной системы Linux, позволяющая нарушителю вызвать отказ в обслуживании	13.11.2025
BDU:2025-15300	Уязвимость интерфейсов cpu_latency_qos_add, remove, update_request модуля drivers/ufs/core/ufs-sysfs.c драйвера поддержки устройств SCSI ядра операционной системы Linux, позволяющая нарушителю вызвать отказ в обслуживании	03.12.2025

Рис. 5. Уязвимости ОС личного компьютера

Базовый вектор уязвимости CVSS 2.0: AV:A/AC:L/Au:S/C:C/I:C/A:C.

AV: A (Access Vector: Adjacent Network) — параметр, указывающий на то, что атакующий должен находиться в той же локальной сети или в непосредственной сетевой близости (например, в одной Wi-Fi сети) для реализации атаки.

AC: L (Access Complexity: Low) — низкая сложность эксплуатации уязвимости. Для успешной атаки не требуется выполнения сложных условий или специальной подготовки среды.

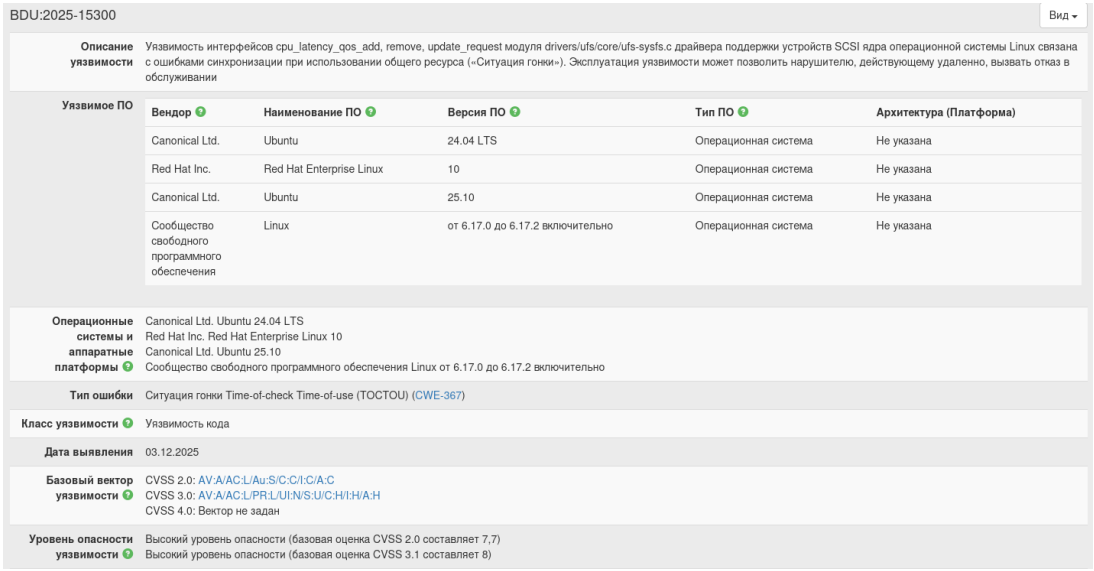
Au: S (Authentication: Single) — для осуществления атаки требуется прохождение аутентификации один раз. Это означает, что атакующий должен обладать учетной записью или иным способом пройти проверку подлинности.

C: C (Confidentiality Impact: Complete) — полное нарушение конфиденциальности. Уязвимость позволяет получить полный доступ к защищаемой информации.

I: C (Integrity Impact: Complete) — полное нарушение целостности. Злоумышленник может изменять или уничтожать данные без ограничений.

A: C (Availability Impact: Complete) — полное нарушение доступности. Эксплуатация уязвимости может привести к отказу в обслуживании или полной недоступности системы.

Уязвимость была устранена в версии 25.10-6.17.0-14.14, поэтому для её устранения достаточно было обновить ОС до этой версии.



BDU:2025-15300

Вид

Описание уязвимости: Уязвимость интерфейсов cpu_latency_qos_add, remove, update_request модуля drivers/ufs/core/ufs-sysfs.c драйвера поддержки устройств SCSI ядра операционной системы Linux связана с ошибками синхронизации при использовании общего ресурса («Ситуация гонки»). Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, вызвать отказ в обслуживании

Уязвимое ПО

Вендор	Наименование ПО	Версия ПО	Тип ПО	Архитектура (Платформа)
Canonical Ltd.	Ubuntu	24.04 LTS	Операционная система	Не указана
Red Hat Inc.	Red Hat Enterprise Linux	10	Операционная система	Не указана
Canonical Ltd.	Ubuntu	25.10	Операционная система	Не указана
Сообщество свободного программного обеспечения	Linux	от 6.17.0 до 6.17.2 включительно	Операционная система	Не указана

Операционные системы и аппаратные платформы:
Canonical Ltd. Ubuntu 24.04 LTS
Red Hat Inc. Red Hat Enterprise Linux 10
Canonical Ltd. Ubuntu 25.10
Сообщество свободного программного обеспечения Linux от 6.17.0 до 6.17.2 включительно

Тип ошибки: Ситуация гонки Time-of-check Time-of-use (TOCTOU) (CWE-367)

Класс уязвимости: Уязвимость кода

Дата выявления: 03.12.2025

Базовый вектор уязвимости:
CVSS 2.0: AV:A/AC:L/Au:S/C:C/I:C/A:C
CVSS 3.0: AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS 4.0: Вектор не задан

Уровень опасности уязвимости:
Высокий уровень опасности (базовая оценка CVSS 2.0 составляет 7,7)
Высокий уровень опасности (базовая оценка CVSS 3.1 составляет 8)

Рис. 6. Развёрнутое описание уязвимости BDU:2025-15300

1.5 Уязвимости ОС личного мобильного устройства

Для поиска уязвимостей ОС личного мобильного устройства на сайте Банка данных угроз безопасности информации ФСТЭК России были использованы следующие критерии:

1. Операционная система: Android 11.
2. Уровень опасности: критический.

По заданным критериям была найдена 1 уязвимость (см. Рис. 7).

BDU:2023-08587	Уязвимость функции callback_thread_event (com_android_bluetooth_btservice_AdapterService.cpp) операционной системы Android, позволяющая нарушителю выполнить произвольный код	01.12.2023

Рис. 7. Уязвимости ОС личного мобильного устройства

Развёрнутое описание уязвимости BDU:2023-08587 «Уязвимость функции callback_thread_event (com_android_bluetooth_btservice_AdapterService.cpp) операционной системы Android связана с использованием памяти после её освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код», представлено на рисунке 8.

Базовый вектор уязвимости CVSS 2.0: AV:N/AC:L/Au:N/C:C/I:C/A:C.

AV: N (Access Vector: Network) — параметр, указывающий на то, что атакующий может осуществить атаку удалённо через сеть (например, через Интернет), без необходимости физического доступа или нахождения в локальной сети.

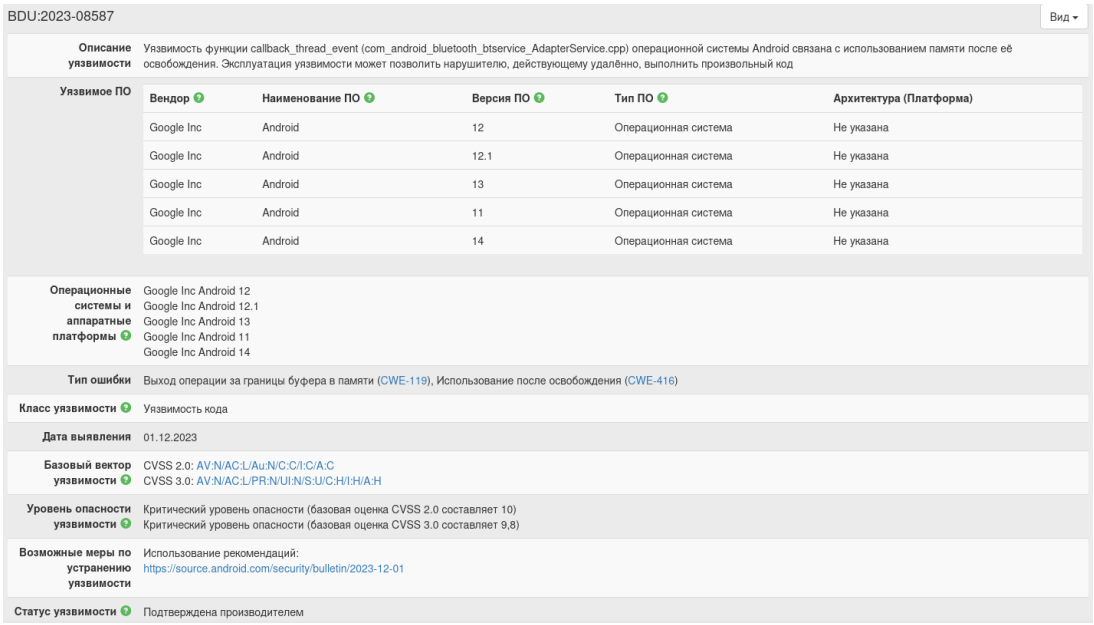
AC: L (Access Complexity: Low) — низкая сложность эксплуатации уязвимости. Для успешной атаки не требуется специальных условий или сложной подготовки.

Au: N (Authentication: None) — для эксплуатации уязвимости не требуется аутентификация. Атакующий может выполнить атаку без наличия учетной записи или прохождения процедуры входа в систему.

C: C (Confidentiality Impact: Complete) — полное нарушение конфиденциальности. Уязвимость позволяет злоумышленнику получить полный доступ к конфиденциальной информации.

I: C (Integrity Impact: Complete) — полное нарушение целостности. Атакующий может изменять, подменять или удалять данные без ограничений.

A: C (Availability Impact: Complete) — полное нарушение доступности. Эксплуатация уязвимости может привести к полной недоступности системы или отказу в обслуживании.



BDU:2023-08587 — Вид

Описание уязвимости: Уязвимость функции callback_thread_event (com_android_bluetooth_btservice_AdapterService.cpp) операционной системы Android связана с использованием памяти после её освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код

Уязвимое ПО

Вендор	Наименование ПО	Версия ПО	Тип ПО	Архитектура (Платформа)
Google Inc	Android	12	Операционная система	Не указана
Google Inc	Android	12.1	Операционная система	Не указана
Google Inc	Android	13	Операционная система	Не указана
Google Inc	Android	11	Операционная система	Не указана
Google Inc	Android	14	Операционная система	Не указана

Операционные системы и аппаратные платформы: Google Inc Android 12; Google Inc Android 12.1; Google Inc Android 13; Google Inc Android 11; Google Inc Android 14

Тип ошибки: Выход операции за границы буфера в памяти (CWE-119), Использование после освобождения (CWE-416)

Класс уязвимости: Уязвимость кода

Дата выявления: 01.12.2023

Базовый вектор уязвимости: CVSS 2.0: AV:N/AC:L/Au:N/C:C/I:C/A:C; CVSS 3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Уровень опасности уязвимости: Критический уровень опасности (базовая оценка CVSS 2.0 составляет 10); Критический уровень опасности (базовая оценка CVSS 3.0 составляет 9,8)

Возможные меры по устранению уязвимости: Использование рекомендаций: https://source.android.com/security/bulletin/2023-12-01

Статус уязвимости: Подтверждена производителем

Рис. 8. Развёрнутое описание уязвимости BDU:2023-08587

Заключение

В ходе выполнения практической работы №1 был проведён анализ уязвимостей программного обеспечения с использованием Банка данных угроз ФСТЭК России. Были изучены структура разделов «Угрозы» и «Уязвимости», определены версии операционных систем личного компьютера и смартфона, а также выполнен поиск уязвимостей с уровнем опасности «Критический» и «Высокий». Проведён анализ наиболее актуальных уязвимостей, рассмотрены их характеристики и векторы CVSS, а также рекомендации по устранению. В процессе выполнения работы были получены практические навыки поиска, анализа и оценки уязвимостей информационных систем.

Список литературы

1. *Федеральная служба по техническому и экспортному контролю Российской Федерации.* Банк данных угроз безопасности информации [Электронный ресурс] / ФСТЭК России. — 2026. — URL: `https://bdu.fstec.ru` (дата обр. 25.02.2026).