ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056
DOI 10.37468/2307-1400-2025-2-49-67

Анализ угроз безопасности и мер защиты информации в компьютерных системах высших учебных заведений

Пшеничный Дмитрий Викторович[1]
Дьяченко Юрий Юрьевич[1]

[1]*Донецкий национальный технический университет, Донецк, Россия*

Аннотация
В статье проведен анализ актуальных киберугроз, направленных против России. Рассмотрены тактики, техники и последствия атак, а также систематизированы основные меры защиты информационных систем от внешних воздействий. Исследование основано на данных ФСБ России, отчетах Positive Technologies и других авторитетных источниках. Предложен алгоритм циклического обновления мер защиты в информационных системах высших учебных заведений.

Ключевые слова: кибербезопасность, фишинг, вредоносное ПО, социальная инженерия, DDoS-атаки, уязвимости, защита данных, киберугрозы, публичные Wi-Fi сети, информационная безопасность, многоуровневый контроль доступа, алгоритм циклического обновления мер защиты.

Введение

Кибератаки на Россию осуществляются с непосредственным участием Пентагона, в этом процессе задействуются как международные (Anonymous, Silence), так и национальные (Ghost Clan – США, RedHack – Турция, GNG – Грузия, Squad 303 – Польша) и менее известные (Cloud Werewolf, TaxOff, Rare Werewolf, Paper Werewolf) хакерские группировки. Финансирование некоторых хакерских группировок происходит через различные киберпреступные действия. Они получают средства от вымогательства, кражи налоговой информации, участия в организованных преступных группах и продажи данных на черном рынке, а также от продажи доступа к облачным сервисам и компрометированным учетным данным.

Об этом сообщили в Центре общественных связей ФСБ России. В ведомстве отметили, что у спецслужбы есть средства для идентификации людей, организаций и реальных заказчиков кибератак на российскую инфраструктуру с целью их привлечения к ответственности.

В ФСБ обратили внимание на то, что Соединенные Штаты стремятся замаскировать свою связь с атаками, выставляя группировку IT Army of Ukraine в качестве их инициаторов. "В процессе анализа обнаруженных киберугроз были получены сведения, указывающие на использование США и стран НАТО украинской территории для проведения масштабных компьютерных атак на гражданские объекты в России", – подчеркивают в ведомстве. Согласно информации от правоохранительных органов, сетевая инфраструктура Украины используется Западом для тайного применения новых типов кибероружия. Федеральной службой безопасности Российской Федерации с начала 2022 года зафиксировано более пяти тысяч хакерских атак на

критическую инфраструктуру России [1]. Несмотря на принимаемые меры, количество успешных кибератак продолжает расти, что требует системного анализа современных угроз и методов защиты.

Научная новизна исследования заключается в:

- классификации уязвимостей российских ОС по данным БДУ ФСТЭК 2024 – 2025 гг;
- анализе современных техник и тактик хакерских группировок (Anonymous, IT Army of Ukraine и др.);
- систематизации мер защиты для каждого типа атак (фишинг, DDoS и пр.);
- предложен алгоритм циклического обновления мер защиты в информационных системах высших учебных заведений.

Практическая значимость работы заключается в:

- конкретных рекомендациях по защите от основных типов угроз;
- методикой анализа уязвимостей для российских ОС;
- материалах для подготовки специалистов по кибербезопасности.

Как показывают исследования, в 2024-2025 годах выявлено шесть основных типов атак, наиболее часто используемых против российских объектов [2]:

- фишинговые атаки;
- вредоносное программное обеспечение (ВПО);
- атаки на системы с использованием уязвимостей;
- социальная инженерия;
- применение бот-сетей;
- эксплуатация публичных Wi-Fi сетей.

Каждый из этих методов имеет свои особенности реализации и требует специфических мер противодействия, что будет рассмотрено в данной статье.

Методы исследования

1. Фишинговые атаки – это вид мошенничества, при котором злоумышленник вынуждает жертву совершить действие, позволяющее получить доступ к устройству, учетным записям или персональным данным. Выступая в роли доверенного лица, мошенник внедряет на компьютер жертвы ВПО или похищает конфиденциальную информацию [3-6].

Тактики:

- маскировка под известные бренды или сервисы используя социальную инженерию для повышения доверия у жертвы, подделка доменов;
- использование срочных призывов к действию, чтобы вызвать паническое поведение у жертвы.

Техники:

- создание поддельных страниц для ввода данных, которые выглядят как официальные сайты;
- генерация ссылок и вложений с использованием URL-редиректов для скрытия настоящего адреса.

Например, в письмах могут содержаться архивы с вредоносными файлами, такими как «СВЕРКА.rar» или ссылки на сервисы, такие как «Яндекс Диск».

Примеры уязвимостей:

- использование простых и предсказуемых паролей, которые легко могут быть угаданы или нарушены;
- недостаточная осведомленность пользователей о вреде фишинга, что делает их более восприимчивыми к манипуляциям;
- использование общедоступных адресов электронной почты, которые могут быть легко подделаны злоумышленниками.

Основные угрозы безопасности и последствия фишинговых атак указаны в Таблице 1.

Таблица 1 – Основные угрозы безопасности и последствия с использованием социальной инженерии

№ п/п	Основные угрозы	Последствия атак
1	Утечка личной информации	- несанкционированный доступ к системам
		- компрометация конфиденциальных данных
2	Финансовые потери	- прямой ущерб от мошенничества
		- затраты на восстановление после атаки
3	Заражение ВПО	- потеря контроля над системами
		- создание ботнетов, шифрование данных
4	Доступ к учётным записям	- кража аккаунтов (почта, банк, корпоративные системы)
5	Репутационный ущерб	- снижение доверия клиентов/партнёров
		- долгосрочные потери имиджа
6	Юридические последствия	- штрафы за нарушение GDPR, 152-ФЗ
		- судебные иски
7	Утрата данных	- остановка бизнес-процессов
		- необходимость восстановления из резервных копий
8	Психологическое воздействие	- стресс и снижение продуктивности сотрудников
9	Дополнительные затраты на защиту	- покупка новых средств безопасности
		- обучение сотрудников
10	Шантаж и вымогательство	- требования выкупа за данные (после утечки)

2. Использование вредоносного программного обеспечения (ВПО) – после открытия вредоносных файлов происходит загрузка и внедрение различных типов ВПО, таких как «трояны удаленного доступа», «шифровальщики», «шпионское ПО», «загрузчики», «майнеры», «банковские трояны», и «другие» (например, Revenge RAT, Remcos RAT, NanoCore RAT, njRAT, Trinper, DarkWatchman, бэкдоры, и т.д.) доля успешных атак с использованием ВПО на момент второго квартала 2024 года приведена в отчете "Positive Technologies" (см. Рисунок 1) [7-9].

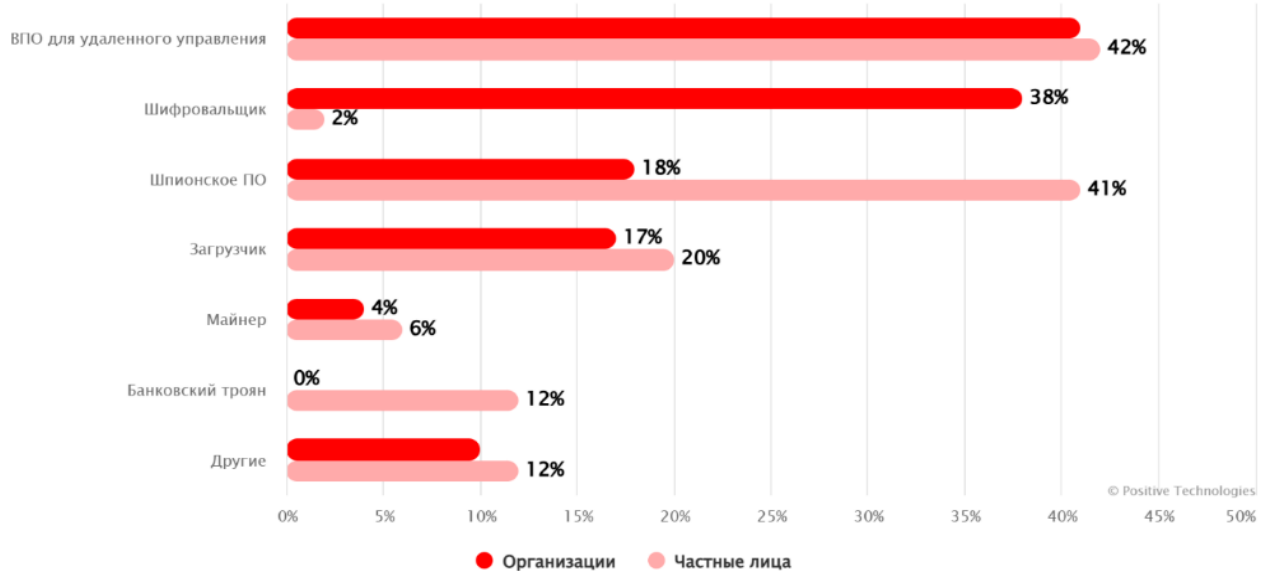

Рисунок 1 – Типы вредоносного ПО (доля успешных атак с использованием ВПО)

Тактики:

- применение «социальной инженерии» для убеждения пользователей открыть зараженные файлы;
- установка программы через скрытые скрипты или эксплойты в уязвимостях системы;
- скрытие вредоносных файлов в законных приложениях или документах.

Техники:

- использование бэкдоров для сохранения доступа к зараженной системе;
- внедрение инструментов для удаленного управления, позволяя злоумышленнику выполнять действия на компьютере жертвы;
- эксплуатация уязвимостей приложений для скачивания и установки зловредного ПО, использование скриптов для автоматизации процессов.

Примеры уязвимостей:

- отсутствие антивирусного программного обеспечения на устройствах пользователей, что позволяет злоумышленникам устанавливать ВПО;
- уязвимости в приложениях, позволяющие выполнять произвольный код или загружать вредоносные файлы;
- ошибки в системах безопасности, которые позволяют обходить защитные механизмы.

Основные угрозы безопасности и последствия использования ВПО указаны в Таблице 2.

Таблица 2 – Основные угрозы безопасности и последствия использования ВПО

№ п/п	Основные угрозы	Последствия атак
1	Кража/утечка данных	- личные данные (пароли, персональная информация)
		- конфиденциальные корпоративные данные
		- финансовая информация (платёжные реквизиты)
2	Повреждение систем	- уничтожение файлов и программного обеспечения
		- нарушение работы ИТ-инфраструктуры
		- необходимость сложного восстановления данных
3	Операционные нарушения	- простой систем и остановка бизнес-процессов
		- снижение производительности рабочих станций
		- дополнительные затраты на аварийное восстановление
4	Распространение инфекции	- заражение других устройств в сети
		- эскалация атаки на смежные системы
		- создание бот-сетей из заражённых компьютеров
5	Скрытые угрозы	- установка бэкдоров для постоянного доступа
		- внедрение шпионских модулей
		- создание каналов утечки данных
6	Шантаж и блокировка	- криптографическое блокирование данных
		- требования выкупа за доступ к системам
		- угрозы публикации украденной информации
7	Репутационные риски	- потеря доверия клиентов
		- ущерб деловой репутации
		- проблемы с регулирующими органами
8	Косвенные последствия	- судебные издержки и штрафы
		- повышение страховых ставок
		- необходимость инвестиций в новые системы защиты

3. Атаки на системы с использованием уязвимостей – злоумышленники исследуют системы на наличие уязвимостей, позволяющих им получить доступ к данным или ресурсам. Это может включать манипуляции с уязвимостями в ПО или сетевой инфраструктуре [10].

Обнаружение уязвимостей – это процесс поиска и исследования уязвимостей в программном обеспечении и аппаратуре, который может быть использован злоумышленником для несанкционированного доступа или нарушения целостности данных. Данный процесс включает в себя широкий спектр методов и технологий, которые помогают выявлять проблемные места в системе и принимать меры для их устранения [11].

Тактики:

- поиск уязвимостей с помощью сканеров и тестов на проникновение;
- использование известных эксплойтов для доступа к системе.

Техники:

- социальная инженерия, заставляющая сотрудников открывать дверь для доступа к уязвимым системам;
- использование инструментов для пентестинга, таких как Metasploit, а также применение SQL-инъекций или XSS-атак;
- проведение атак на основе предыдущих данных об уязвимостях, выявленных в системах и приложениях.

Примеры уязвимостей:

- устаревшие версии программного обеспечения, которые создают потенциальные двери для злоумышленников;
- недостатки в процессах аутентификации, позволяющие нарушить защиту пользователей;
- неверные конфигурации сетевых устройств, что может предоставить доступ к защищённой информации.

Основные угрозы безопасности и последствия атаки на системы с использованием уязвимостей указаны в Таблице 3.

Таблица 3 – Основные угрозы безопасности и последствия атаки на системы с использованием уязвимостей

№ п/п	Основные угрозы	Последствия атак
1	Несанкционированный доступ	– утечка конфиденциальной информации
		– кража/уничтожение данных (включая интеллектуальную собственность)
2	Внедрение вредоносного ПО (ВПО)	– заражение систем и сетей
		– создание скрытых бэкдоров для дальнейших атак
3	Атаки типа "отказ в обслуживании" (DDoS)	– нарушение доступности сервисов
		– финансовые потери из-за простоя
4	Потеря/уничтожение данных	– утрата критически важной информации
		– повреждение баз данных и резервных копий
5	Финансовые убытки	– затраты на восстановление систем
		– штрафы за нарушение соответствия (GDPR, PCI DSS)
6	Репутационный ущерб	– потеря доверия клиентов и партнёров
		– снижение рыночной стоимости компании
7	Утрата конкурентных преимуществ	– кража коммерческой тайны
		– копирование технологий конкурентами

4. Социальная инженерия – злоумышленники используют психологические приемы для того, чтобы обмануть жертв, заставляя их раскрывать конфиденциальную информацию или

выполнять определенные действия, направленные на снижение их безопасности. Это метод воздействия на людей, направленный на получение их личной информации, доступа к ресурсам или других ценных объектов [12-15]. Киберпреступники мастерски владеют искусством обмана: они умеют убеждать ничего не подозревающих пользователей поделиться своими данными, инфицировать системы вредоносным программным обеспечением или предоставить доступ к системам, которые не предназначены для внешних пользователей [12-15].

Тактики:

- использование доверительных отношений и манипуляции психологическим состоянием жертвы для получения необходимой информации;
- создание фальшивых сценариев, таких как помощь в решении проблемы или предложение выгодного сотрудничества.

Техники:

- телефонные звонки под видом официальных представителей для сбора конфиденциальных данных;
- фальшивые электронные письма, имитирующие внутренние коммуникации компании, для побуждения сотрудников к действию;
- фишинг через SMS-сообщения (smishing) для получения личной информации.

Примеры уязвимостей:

- недостаточная подготовленность сотрудников к выявлению и противодействию манипуляциям;
- доверительность организаций, позволяющая злоумышленникам входить в доверие к сотрудникам;
- отсутствие системы проверки идентичности для критически важных запросов, повышающих риски компрометации данных.

Основные угрозы безопасности и последствия с использованием социальной инженерии указаны в Таблице 4.

Таблица 4 – Основные угрозы безопасности и последствия с использованием социальной инженерии

№ п/п	Основные угрозы	Последствия атак
1	Утечка конфиденциальных данных	- раскрытие важной информации (пароли, финансовая информация);
		- компрометация персональных данных клиентов и сотрудников;
2	Манипулирование пользователями	- несанкционированный доступ к учетным записям;
		- получение злоумышленниками привилегированных прав;
3	Финансовые потери	- прямая кража денежных средств;
		- затраты на восстановление после атаки;
4	Несоответствие регуляторным требованиям	- нарушение GDPR, ФЗ-152 и других нормативов;
		- юридическая ответственность;
5	Репутационные риски	- потеря доверия клиентов;
		- ухудшение имиджа компании;
		- уход бизнес-партнеров;
6	Дальнейшие угрозы безопасности	- распространение атаки на другие системы;
		- установка вредоносного ПО;
		- кибершпионаж

5. Применение бот-сетей – злоумышленники могут контролировать большое количество устройств для выполнения атак, таких как DDoS, с целью перегрузки и выведения из строя серверов. DDoS-атака (Distributed Denial of Service, распределенная атака типа "отказ в обслуживании") – это кибератака, цель которой заключается в том, чтобы сделать ресурс

(например, веб-сайт или сетевую службу) недоступным для его законных пользователей. Осуществляется это путем перегрузки целевой системы огромным количеством запросов, превышающих ее обработочные возможности [16, 17].

Данный вид атаки может привести к различным серьезным последствиям, включая:

- DDoS-атаки: использование бот-сетей для перегрузки серверов может привести к временной неработоспособности услуг;
- простои в обслуживании: атаки могут вызвать значительные задержки и остановки в работе онлайн-сервисов, что сказывается на пользователях;
- широкий масштаб атак: бот-сети могут одновременно атаковать множество целей, увеличивая урон от атак;
- увеличение затрат на защиту: необходимость защиты от бот-сетей требует дополнительных ресурсов и инвестиций со стороны организаций.

Бот-сети представляют собой значительную угрозу для онлайн-ресурсов, требуя комплексного подхода к защите и мониторингу трафика.

Тактики:

- заражение устройств вирусами для создания бот-сетей с целью дальнейшего использования в атаках;
- координация атаки на целевые серверы с помощью распределенных узлов из зараженных устройств.

Техники:

- использование командно-управляющих серверов (C&C) для контроля над ботами;
- установка различных видов ВПО на ботах для выполнения разных задач, включая кражу данных или DDoS-атаки;
- эмуляция обычного трафика для маскировки действий бот-сетей от систем защиты.

Примеры уязвимостей:

- недостаточная защита устройств IoT, которые могут быть легко захвачены для создания бот-сетей;
- уязвимости в безопасности домашних сетей, позволяющие злоумышленникам получить доступ к пользователям и их устройствам;
- недостаточно защищённые приложения, которые могут стать точками входа для создания бот-сетей.

Основные угрозы безопасности и последствия применения бот-сетей указаны в Таблице 5.

Таблица 5 – Основные угрозы безопасности и последствия применения бот-сетей

№ п/п	Основные угрозы	Последствия атак
1	Перехват данных	- доступ злоумышленников к паролям, финансовым данным
		- кража конфиденциальной информации
2	Заражение устройств ВПО	- установка троянов, шпионского ПО
		- потеря контроля над устройством
3	Взлом учетных записей	- несанкционированный доступ к аккаунтам
		- кража цифровой идентичности
4	Угрозы корпоративной безопасности	- утечка служебных данных
		- компрометация внутренних систем компании
5	Финансовые убытки	- прямые потери денежных средств
		- расходы на восстановление после атаки
6	Компрометация устройств	- полный контроль злоумышленников над устройством
		- использование устройства для новых атак
7	Потеря доверия к компании	- репутационный ущерб
		- отток клиентов

6. Эксплуатация публичных Wi-Fi сетей - злоумышленники могут перехватывать данные пользователей в общественных сетях, используя специальные инструменты для отслеживания сетевого трафика и получения конфиденциальной информации.

Wi-Fi – технология беспроводной локальной сети с устройствами на основе стандартов IEEE 802.11. В настоящее время данная аббревиатура охватывает стандарты передачи цифровых данных через радиоканалы. Wi-Fi считается относительно новой и одной из наиболее перспективных технологий в сфере компьютерной связи. В 1998 году инженер Джон О'Салливан разработал беспроводной протокол передачи данных. На сегодняшний день существует уже шесть поколений Wi-Fi, последнее из которых было анонсировано в 2019 году. Изначально эта технология предназначалась для использования в корпоративных сетях с целью замены проводных решений. Проводные сети требуют тщательной разработки топологии и прокладки значительных расстояний кабеля, что является довольно затратным процессом. Но, как все мы знаем, сегодня Wi-Fi применяется во многих сферах [18-20].

В современных условиях технология Wi-Fi позволяет подключаться к интернету по беспроводному каналу в зоне покрытия точки доступа. Такие публичные зоны с высокоскоростным интернетом известны как Hotspot. На Рисунке 2 представлена схема типичной точки доступа [18-20].

Рисунок 2 – Организация хотспота

Эксплуатация публичных Wi-Fi сетей может привести к различным серьезным последствиям, включая:

- перехват данных: злоумышленники могут получать доступ к передаваемой информации, включая пароли и данные о финансовых транзакциях;
- угроза безопасности устройств: использование публичных сетей может привести к заражению устройств ВПО;
- ущерб для пользователей: жертвы атак могут потерять деньги, идентификацию или конфиденциальную информацию;
- потеря доверия: компании могут потерять репутацию, если клиенты станут жертвами атак в процессе работы с их сервисами, связанными с общедоступными сетями.

Использование публичных Wi-Fi сетей требует осторожности, поскольку последствия атак могут нанести серьезный ущерб как пользователям, так и организациям.

Тактики:

- создание поддельных точек доступа, имитирующих легитимные сети для перехвата данных пользователей;
- использование снифферов для анализа трафика и сбора конфиденциальной информации.

Техники:

- внедрение методов «человека посередине» (MITM) для перехвата и манипуляции данными между пользователем и сервисами;

- использование сессий кражи (session hijacking) для доступа к учетным записям пользователей;
- установка шпионских программ на устройствах жертв для получения доступа к их информации.

Основные угрозы безопасности и последствия эксплуатации публичных Wi-Fi сетей указаны в Таблице 6.

Таблица 6 – Основные угрозы безопасности и последствия эксплуатации публичных Wi-Fi сетей

№ п/п	Основные угрозы	Последствия атак
1	Перехват данных	- Доступ злоумышленников к паролям, финансовым данным
		- Кража конфиденциальной информации
2	Заражение устройств ВПО	- Установка троянов, шпионского ПО
		- Потеря контроля над устройством
3	Взлом учетных записей	- Несанкционированный доступ к аккаунтам
		- Кража цифровой идентичности
4	Угрозы корпоративной безопасности	- Утечка служебных данных
		- Компрометация внутренних систем компании
5	Финансовые убытки	- Прямые потери денежных средств
		- Расходы на восстановление после атаки
6	Компрометация устройств	- Полный контроль злоумышленников над устройством
		- Использование устройства для новых атак
7	Потеря доверия к компании	- Репутационный ущерб
		- Отток клиентов

7. Классификации уязвимостей ОС по данным БДУ ФСТЭК

В ходе исследования методов кибератак были выявлены и классифицированы уязвимости, эксплуатируемые злоумышленниками в зависимости от целевой операционной системы. Для систематизации данных они распределены по трём категориям: «Linux», «Windows» и «ОС не определена». Такой подход позволяет оценить распределение угроз по платформам, а также выделить случаи, требующие дополнительного анализа [21].

Детализированный перечень уязвимостей представлен в Таблицах 7-9 (Уязвимости Linux в Таблице 7, уязвимости Windows в Таблице 8, уязвимости неопределенных ОС в Таблице 9).

Таблица 7 – Уязвимости Linux

№ п/п	Уязвимость	ОС / ПО	Банк данных угроз безопасности информации	Уровень опасности по CVSS 3.0	Описание	Эксплуатация уязвимости нарушителем
1	Функция ksmbd_vfs_stream_read() демона KSMBD	- Linux - Ubuntu (20.04, 22.04, 24.04) LTS - Debian GNU/Linux 12 - РЕД ОС 7.3 - Ubuntu 24.10	BDU:2025-00883	Критический	Связанная с выходом операции за границы буфера в памяти.	Удаленно, раскрыть защищаемую информацию и вызвать отказ в обслуживании путем отправки специально сформированных SMB-запросов к файлам с ADS.
2	Функция rfcomm_check_security() в модуле net/bluetooth/rfcomm/core.c драйвера bluetooth	- Linux; - ОСОН ОСнова Onyx до 2.10.1	BDU:2024-00986	Средний	Связанная с разыменованием нулевого указателя.	Вызвает отказ в обслуживании.

№ п/п	Уязвимость	ОС / ПО	Банк данных угроз безопасности информации	Уровень опасности по CVSS 3.0	Описание	Эксплуатация уязвимости нарушителем
3	Функции nf_tables_abort() в модуле net/netfilter/nf_tables_api.c компоненты netfilter	- Linux - АО «ИВК» Альт 8 СП - АО «ИВК» АЛЬТ СП 10 - АО "НППКТ" ОСОН ОСнова Onyx до 2.10.1	BDU:2024-04369	Высокий	Связанная с некорректной блокировкой ресурса.	Оказать воздействие на конфиденциальность, целостность и доступность защищаемой информации.

Таблица 8 – Уязвимости Windows

№ п/п	Уязвимость	ОС / ПО	Банк данных угроз безопасности информации	Уровень опасности по CVSS 3.0	Описание	Эксплуатация уязвимости нарушителем
1	Реализации протокола аутентификации NTLMv2	- Windows	BDU:2024-09487	Средний	Связанная с раскрытием хешей в результате некорректного внешнего управления именем или путем файла.	Удаленно, реализовывается атака Pass-the-hash.
2	Драйвер Windows Common Log File System (CLFS)	- Windows	BDU:2024-11011	Высокий	Связанная с переполнением буфера в динамической памяти.	Повышение своих привилегий до уровня SYSTEM.
3	Реализации протокола службы каталогов LDAP	- Windows	BDU:2024-11018	Критический	Связанная с целочисленным переполнением.	Удаленно, выполнить произвольный код.

Таблица 9 – Уязвимости (ОС не определена)

№ п/п	Уязвимость	ОС / ПО	Банк данных угроз безопасности информации	Уровень опасности по CVSS 3.0	Описание	Эксплуатация уязвимости нарушителем
1	Протоколы туннелирования пакетов IPv4-in-IPv6 и IPv6-in-IPv4	Данные уточняются	BDU:2025-00420	Высокий	Связанная с недостаточной проверкой источника канала связи.	Удаленно, реализовать атаки типа «подмена доверенного объекта» путем отправки специально сформированного пакета с двумя IP-заголовками.
2	Сервиса для управления бизнесом Битрикс24 и системы управления содержимым сайтов (CMS) 1С-Битрикс: Управление сайтом.	Данные уточняются	BDU:2025-00765	Высокий	Связанная с непринятием мер по защите структуры веб-страницы.	Удаленно, выполнить произвольный код путем отправки специально сформированного HTTP-запроса.
3	Пакетов программ Microsoft Office, Excel и 365 Apps for Enterprise	Данные уточняются	BDU:2025-01553	Высокий	Связанная с разыменованием недоверенного указателя.	Выполнение произвольного кода.

Результаты исследования

Меры для повышения безопасности

В ходе исследования были рассмотрены типы атак, наиболее часто используемые злоумышленниками. Анализируя уязвимости, которые позволяют злоумышленникам успешно провести рассмотренные атаки можно сформулировать основные меры, направленные на защиту от угроз безопасности информации.

С целью повышения безопасности объектов информатизации определены основные меры защиты, актуальные для большинства угроз:

1. Обучение сотрудников – регулярные тренинги по кибербезопасности, повышение осведомленности о различных угрозах.
2. Регулярное обновление программного обеспечения – установка патчей и обновлений для устранения уязвимостей [22].
3. Использование антивирусного ПО и файрволлов – защита от вредоносного ПО и несанкционированного доступа.
4. Многофакторная аутентификация (MFA) – дополнительный уровень защиты для доступа к системам.
5. Мониторинг сетевой активности – выявление аномалий и подозрительных действий.
6. Ограничение прав доступа – принцип минимальных привилегий для пользователей.

При этом следует выполнить дополнительные меры защиты, специфичные для определенного типа атак, дополняющие базовые меры защиты:

1. Фишинговые рассылки:
   - настройка системы мониторинга событий ИБ (включение индикаторов компрометации, таких как хеши SHA256);
   - ограничение обращений к подозрительным адресам (использование черных/белых списков);
   - внедрение политики управления паролями (строгие требования к сложности и смене паролей).
2. Использование вредоносного программного обеспечения:
   - проведение регулярных обследований сети на наличие ВПО;
   - регулярные резервные копии данных для восстановления после заражения;
   - использование систем обнаружения вторжений (IDS/IPS).
3. Атаки на системы с использованием уязвимостей:
   - проведение тестов на проникновение (пентесты);
   - внедрение систем обнаружения и предотвращения вторжений (IDS/IPS);
   - настройка строгого контроля доступа к критическим системам.
4. Социальная инженерия:
   - создание политики безопасности информации (правила обращения с конфиденциальными данными);
   - проверка личности собеседника перед раскрытием информации;
   - модерирование взаимодействия с клиентами для предотвращения манипуляций;
   - программа реагирования на инциденты социальной инженерии.
5. Бот-сети:
   - установка систем защиты от DDoS-атак;
   - мониторинг сетевого трафика для выявления бот-активности.
   - ограничение доступности ресурса (использование балансировки нагрузки).
6. Публичные Wi-Fi сети:
   - использование VPN для шифрования трафика;
   - ограничение подключений к неопознанным Wi-Fi сетям;
   - отключение общего доступа к файлам при использовании публичных сетей.

Таким образом, защита от рассмотренных киберугроз требует комбинации универсальных и специализированных мер. Ключевыми элементами являются:

- регулярное обучение сотрудников для противодействия социальной инженерии и фишингу.
- многоуровневая техническая защита (обновления, MFA, мониторинг, антивирусы).
- чёткие организационные процедуры (управление доступом, политики безопасности, реагирование на инциденты).

Комплексный подход, сочетающий эти направления, значительно снижает риски для всех категорий атак. Несмотря на эффективность предложенных мер, современные киберугрозы требуют не только статических решений, но и динамической адаптации к новым вызовам. Для этого предлагается внедрение интеллектуальных систем, способных автоматизировать процессы обнаружения, анализа и нейтрализации атак. С учетом появления новых угроз безопасности информации, необходимо проводить комплекс мероприятий, направленных на совершенствование системы защиты. Для достижения этой цели авторами предложен алгоритм циклического обновления защиты, выполняющий следующие процедуры:

- многоуровневый контроль доступа;
- непрерывный мониторинг аномалий;
- автоматизированная корректировка мер защиты на основе рекомендаций ФСТЭК.

Многоуровневый контроль доступа включает четыре ключевых уровня защиты, каждый из которых выполняет строго определенные функции (Рисунок 3).

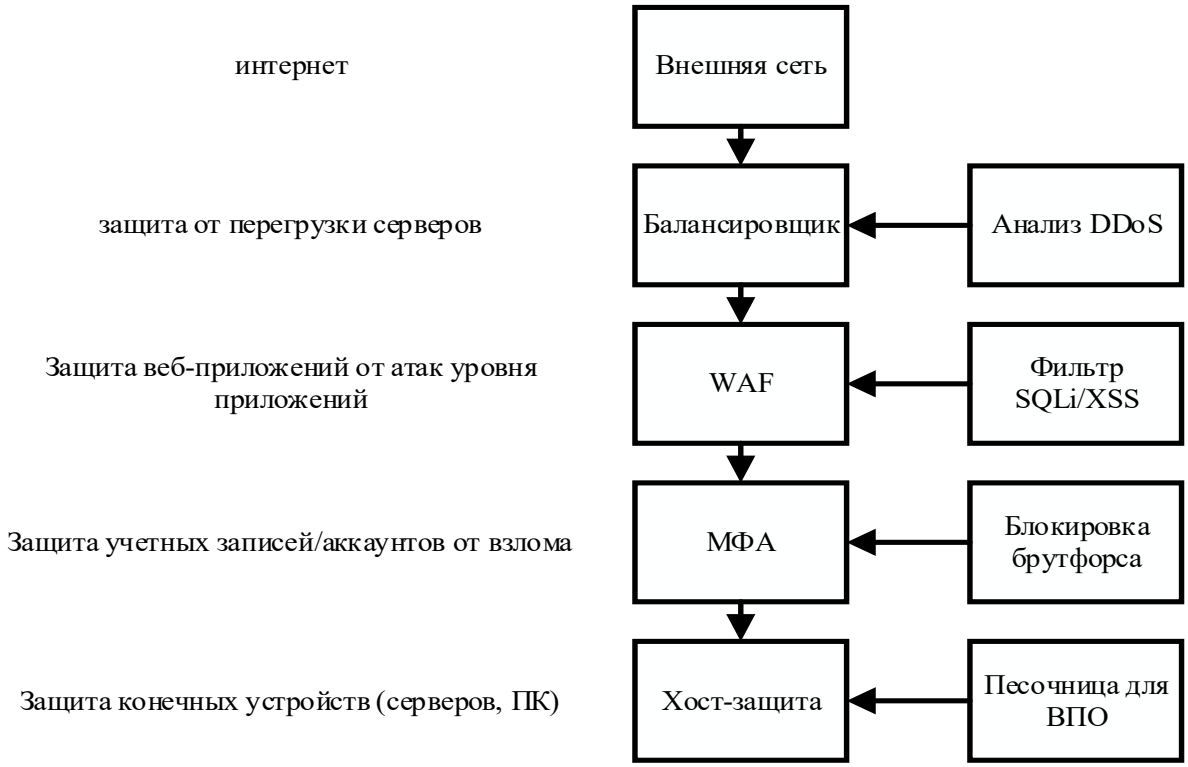

Рисунок 3 – Многоуровневый контроль доступа

Непрерывный мониторинг аномалий представлен на рисунке 4 (блок 1). Данная процедура предусматривает, что после запуска программа работает непрерывно и не требует дополнительных вмешательств. При поступлении "атаки" происходит ее обнаружение, путём "Улучшение детекции" (добавление новых правил: повышение уровня чувствительности, обновление баз сигнатур или моделей машинного обучения, анализ ложных).

Автоматизированная корректировка мер защиты на основе рекомендаций ФСТЭК представлена на рисунке 4 (блок 2). При обнаружении успешной атаки система выполняет следующие процедуры.

1. Анализ прорыва атаки.
2. Поиск соответствующих уязвимостей в реестре БДУ ФСТЭК.
3. Генерация новых правил защиты, патчинг ПО/ОС.
4. Валидация новых правил защиты в тестовой среде.
5. Внедрение в контур защиты.

Примером можно рассмотреть ситуацию при эксплуатации уязвимости CVE-2024-56627 (BDU:2025-00883) в Linux система автоматически добавляет правило блокировки для уязвимости ksmbd и ставит в очередь обновление пакета.

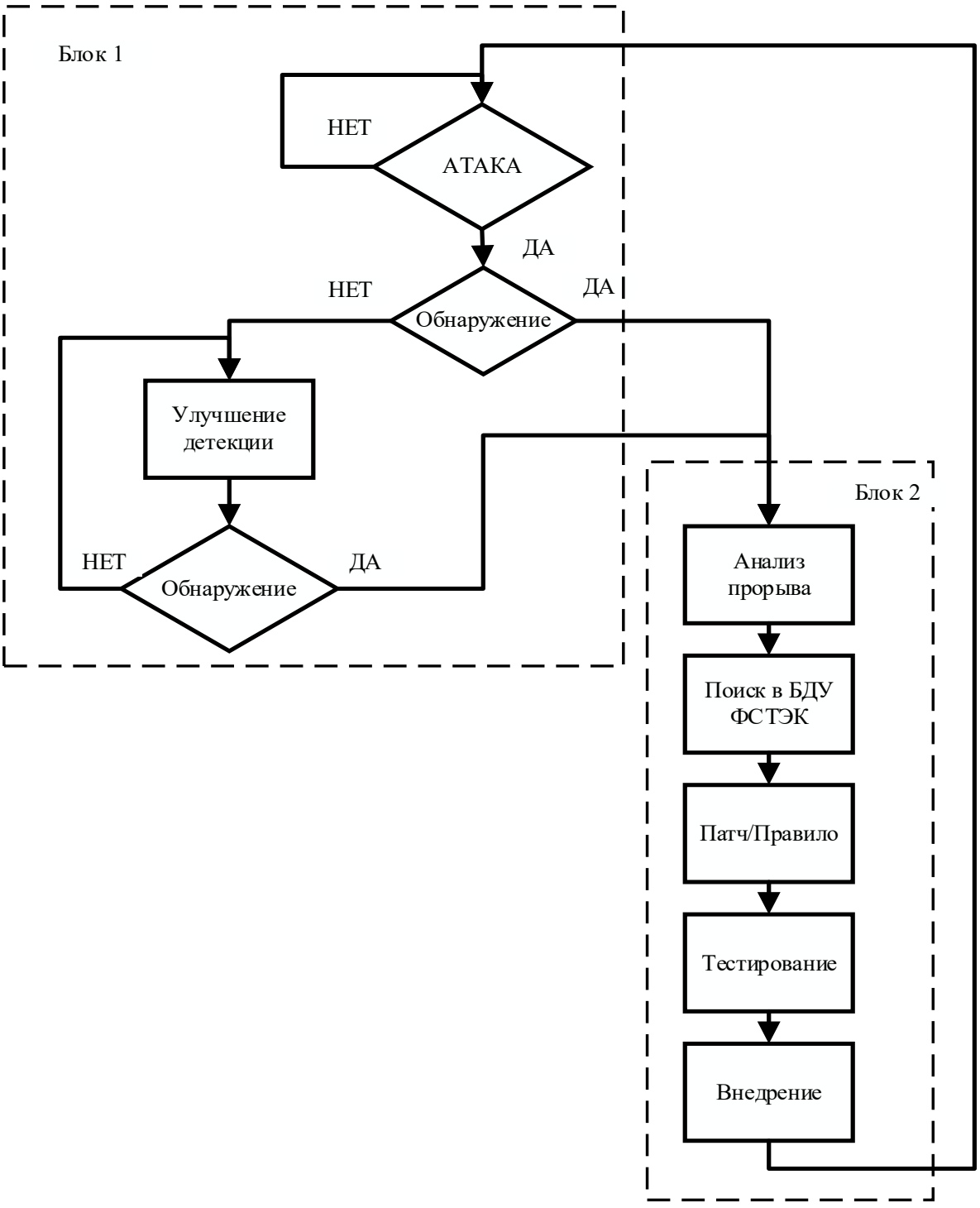

Рисунок 4 – Циклическое обновление защиты в ИС

Алгоритм циклического обновления защиты демонстрирует общий подход к построению адаптивной системы защиты информации, при этом необходимо учитывать, что для успешного отражения конкретных сценариев атак требуется индивидуальный подбор методов их обнаружения. К таким методам можно отнести байесовские и нейронные сети, метод нечетких когнитивных карт, метод онтологии и другие.

Первый алгоритм демонстрирует общий подход к адаптивной защите, однако для работы с конкретными сценариями атак требуется более детализированная стратегия. Второй алгоритм предлагает пошаговый механизм, который позволяет не только обнаруживать угрозы, но и анализировать их источники, а также автоматизировать устранение уязвимостей. Такой комбинированный подход обеспечивает гибкость системы: если первый алгоритм задает общие рамки защиты, то второй предоставляет инструменты для точного реагирования на уникальные случаи. Рассмотрим его структуру на вымышленном примере атаки группировки Cloud Werewolf.

Алгоритм «Поиск уязвимостей и автономное обновление защиты ИС», пошаговый механизм работы:

1. Детекция атаки (как обнаруживаем):
   - SIEM-системы (Splunk/QRadar);
   - аномалии сетевого трафика;
   - логи IDS/IPS (Suricata/Snort);
   - отчеты сотрудников (через обучение).
2. Анализ прорыва

Работа алгоритма представлена на Рисунке 5.

3. Пример для конкретной атаки, легенда компании:
   - группировка "Cloud Werewolf" в Ubuntu Linux (BDU:2025-00883);
   - атака прошла все слои защиты.

Действия системы:

1) Обнаружение через:
   - аномальную нагрузку на демона KSMBD;
   - попытку выполнения shell-кода.
2) Автоматический запрос в БДУ по:
   - ОС: Ubuntu Linux 24.10;
   - сервис: демон KSMBD.
3) Получение патча:

"id" "BDU:2025-00883",
"патч": " 24.10 oracular Fixed 6.11.0-21.21 ",
"мера действия": "Блокировка SMB-запросов к файлам с ADS"

4) Автоматическое применение:
   - добавление правила в фаервол;
   - очередь на обновление через CI/CD.

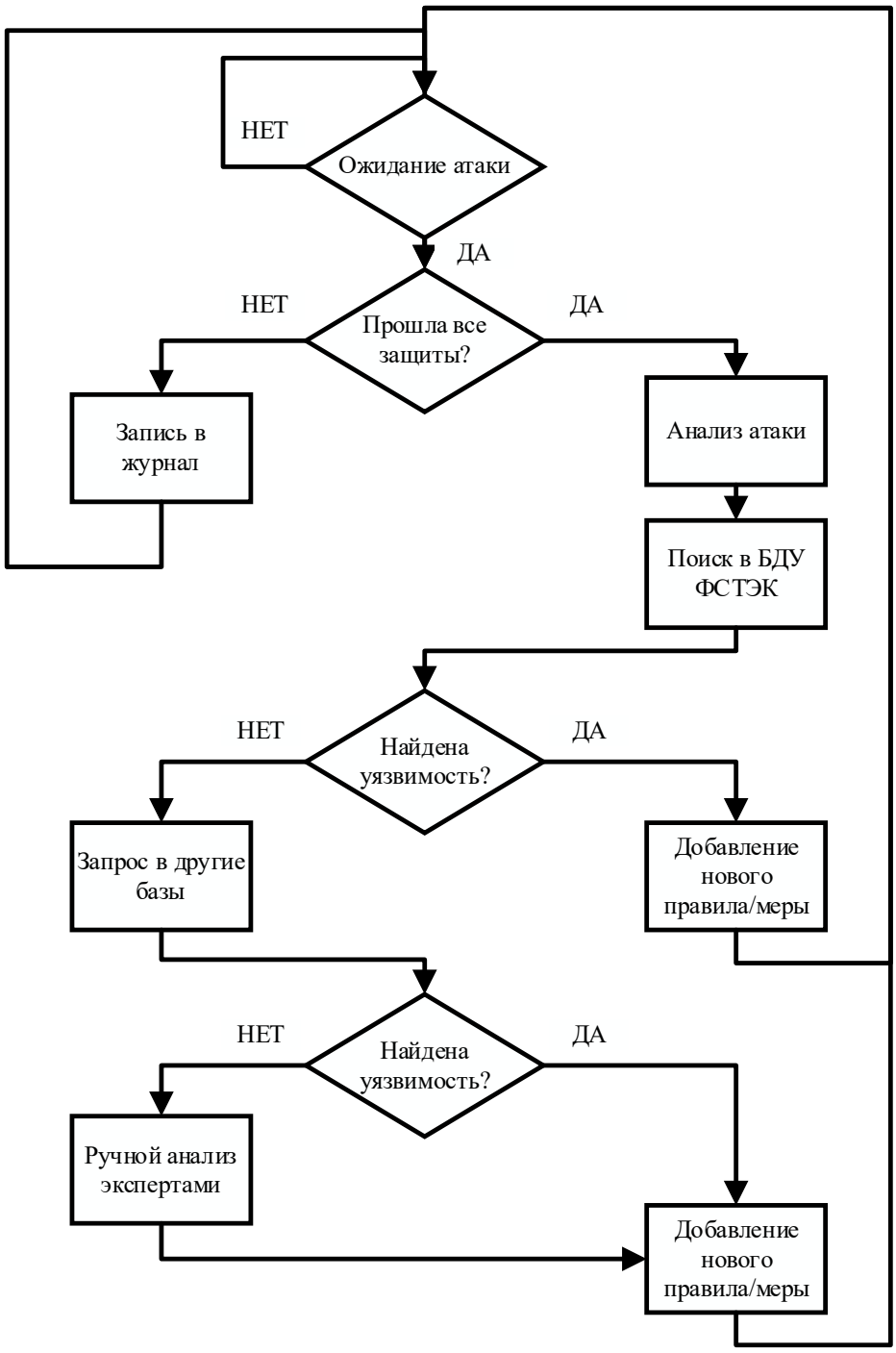

Рисунок 5 – Поиск уязвимостей и автономное обновление защиты ИС

Заключение

В данной статье авторы провели анализ современных киберугроз, направленных против России, включая фишинг, вредоносное ПО, эксплуатацию уязвимостей, социальную инженерию, DDoS-атаки и риски публичных Wi-Fi сетей. На основе данных ФСБ России, отчетов Positive Technologies и других источников систематизировали тактики, техники и последствия атак, а также разработали меры защиты для каждой угрозы.

Ключевые результаты:

1. Классификация уязвимостей российских ОС по данным БДУ ФСТЭК (2024–2025 гг.), что позволяет точнее прогнозировать и предотвращать атаки.

2. Анализ методов работы хакерских группировок, включая Anonymous, IT Army of Ukraine и другие, с выявлением их источников финансирования.

3. Разработка практических рекомендаций по защите, включая обучение сотрудников, обновление ПО, MFA и мониторинг сетевой активности.

4. Предложены алгоритмы циклического обновления мер защиты в информационных системах.

Практическая значимость:

- предложенные меры могут быть внедрены в организациях для снижения рисков кибератак;
- материалы статьи полезны для подготовки специалистов по кибербезопасности.

Исследование подтверждает необходимость комплексного подхода к киберзащите, сочетающего технические, организационные и образовательные меры. Дальнейшая работа будет направлена на адаптацию предложенных алгоритмов под конкретные инфраструктуры и анализ новых угроз. Вопросы построения и совершенствования адаптивных алгоритмов, использующих вышеназванные методы и предназначенных для совершенствования систем защиты информации в информационных системах высших учебных заведений, являются направлением дальнейших исследований авторов.

Список литературы

1. Федеральная служба безопасности Российской Федерации. Официальное сообщение "ФСБ России с начала 2022 года зафиксировано более пяти тысяч хакерских атак на критическую инфраструктуру Российской Федерации" от 13 апреля 2023 г. [Электронный ресурс]. – URL: http://www.fsb.ru/fsb/press/message/single.htm!id=10439694@fsbMessage.html (дата обращения: 17.03.2025).

2. Kaspersky Cyber Threat Intelligence. Ландшафт киберугроз для России и СНГ 2024: аналитический отчет / Н. Назаров, Н. Шорникова, В. Бурцев [и др.] – Kaspersky, 2024. – 121 с. [Электронный ресурс]. – URL: https://www.kaspersky.ru/go/threat-landscape (дата обращения: 04.04.2025).

3. Полное руководство по фишинговым атакам // Хабр. – 2021. – 25 февр. [Электронный ресурс]. – URL: https://habr.com/ru/companies/varonis/articles/544140/ (дата обращения: 18.03.2025).

4. Фишинговые письма: как их распознать и не стать их жертвой // Kaspersky. – 2023. – [Электронный ресурс]. – URL: https://www.kaspersky.ru/resource-center/preemptive-safety/phishing-prevention-tips (дата обращения: 19.03.2025).

5. Бударный Г.С., Дюсметова А.А., Казанцев А.А., Красов А.В. Социальная инженерия: её методы и способы защиты // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023): Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т., Санкт-Петербург, 28 февраля – 01 2023 года. Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023. – С. 200-204. – EDN PWVWPZ.

6. Матвеев Д.В. Фишинг в эпоху цифровизации: методы и стратегии защиты // Тенденции развития науки и образования. – 2024. – № 115-6. – С. 110-115. – DOI 10.18411/trnio-11-2024-262. – EDN MSYLUK.

7. Актуальные киберугрозы: I квартал 2024 года // Positive Technologies. – 2024. – 22 мая [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2024-q1/ (дата обращения: 21.03.2025).

8. Стрельцов Д. Актуальные киберугрозы: II квартал 2024 года // Positive Technologies. – 2024. – 22 авг. [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-ii-kvartal-2024-goda/#id2 (дата обращения: 21.03.2025).

9. Голушко А. Актуальные киберугрозы: IV квартал 2024 года – I квартал 2025 года / А. Голушко // Positive Technologies. – 2025. – 20 марта [Электронный ресурс]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/ (дата обращения: 01.04.2025).

10. Центральный банк Российской Федерации. Attack 2024: [отчет] / Банк России. – Москва, 2024. – 50 с. [Электронный ресурс]. – URL: https://cbr.ru/Collection/Collection/File/55129/Attack_2024.pdf (дата обращения: 04.04.2025).

11. Методы обнаружения уязвимостей в системах безопасности // Hanston. – 2024. – 29 февр. [Электронный ресурс]. – URL: https://hanston.ru/press-centr/metody-obnaruzheniya-uyazvimostej-v-sistemah-bezopasnosti/ (дата обращения: 22.03.2025).

12. Что такое социальная инженерия? // Kaspersky. – 2023. [Электронный ресурс]. – URL: https://www.kaspersky.ru/resource-center/definitions/what-is-social-engineering (дата обращения: 23.03.2025).

13. Протодьяконова А.В., Дмитриева А.Н. Информационная безопасность и интернет // Актуальные вопросы современной науки: теория, методология, практика, инноватика : Сборник научных статей по материалам XIII Международной научно-практической конференции, Уфа, 17 ноября 2023 года. – Уфа: Научно-издательский центр "Вестник науки", 2023. – С. 228-231. – EDN ZKRMYA.

14. Жероков З.А., Георгиев И.С. Информационная безопасность в социальных сетях // Актуальные вопросы современного образования : Сборник научных трудов. – Киров : Межрегиональный центр инновационных технологий в образовании, 2024. – С. 78-80. – EDN CKZYJL.

15. Ермаков М.Г. «Телефонное» мошенничество // Проблемы борьбы с преступностью в условиях цифровизации: теория и практика : Сборник статей XVIII Международной научно-практической конференции, Барнаул, 29 июня 2020 года / Отв. редакторы С.И. Давыдов, В.В. Поляков. Том Выпуск XVI. – Барнаул: Алтайский государственный университет, 2020. – С. 51-55. – EDN CQTEFK.

16. Что такое DDoS-атаки и как оператору связи защититься от них // VAS Experts. – 2024. – 11 янв. [Электронный ресурс]. – URL: https://vasexperts.ru/blog/dpi/chto-takoe-ddos-ataki-i-kak-ot-nih-zashhititsya-operatoru-svyazi/ (дата обращения: 24.03.2025).

17. Бондарев В.В. Введение в информационную безопасность автоматизированных систем: учеб. пособие. – 3-е изд. – Москва: Изд-во МГТУ им. Н. Э. Баумана, 2021. – 252 с.: ил. – ISBN 978-5-7038-5541-6. – EDN BGPOQZ. [Электронный ресурс]. – URL: https://rucont.ru/efd/808476 (дата обращения: 04.04.2025).

18. Паршакова М.С., Успенский Н.К. Анализ угроз и рисков использования публичных локальных беспроводных сетей Wi-Fi // Фундаментальные и прикладные научные исследования: актуальные вопросы, достижения и инновации: сб. ст. XXXIX Междунар. науч.-практ. конф. – Пенза: Наука и Просвещение, 2020. – С. 19–25. – EDN KHQLTA.

19. Скатков А.В., Брюховецкий А.А., Моисеев Д.В., Сухарев Н.В. Модели распределении ресурсов защиты для смягчения отказов узлов на основе метода вектора спада в условиях действия атак в сетях 5G атипичная // Известия Тульского государственного университета. Технические науки. – 2023. – № 7. – С. 512-518. – DOI 10.24412/2071-6168-2023-7-512-513. – EDN TKHXXG.

20. Трусильников С.В. Организация беспроводной локальной вычислительной сети для ООО «Томская транковая компания» // Научная сессия ТУСУР–2009: мат-лы Всерос. науч.-техн. конф. – Томск: В-Спектр, 2008. – Ч. 2. – С. 192–194.

21. Долгопятов А.Ю., Долгопятов О.А. Уязвимости программного обеспечения // Межотраслевые исследования как основа развития научной мысли : Сборник статей Международной научно-практической конференции в 2 частях, Оренбург, 27 декабря 2022 года. Том Часть 1. – Уфа: Общество с ограниченной ответственностью "ОМЕГА САЙНС", 2022. – С. 60-67. – EDN WKFGBS.

22. Шемсетдинов С.Я., Джанмырадов А., Довлетова Г.Я., Базаров Б.З. Предоставление рекомендаций по усилению сетевой безопасности // Тенденции, факторы и механизмы повышения результативности Отечественной науки : Сборник статей Национальной (Всероссийской) научно-практической конференции с международным участием, Воронеж, 22 сентября 2024 года. – Уфа: ООО "Омега сайнс", 2024. – С. 45-47. – EDN KPSQQC.

Статья поступила в редакцию 7 апреля 2025 г.
Принята к публикации 21 июня 2025 г.

Ссылка для цитирования: Пшеничный Д.В., Дьяченко Ю.Ю. Анализ угроз безопасности и мер защиты информации в компьютерных системах высших учебных заведений // Национальная безопасность и стратегическое планирование. 2025. № 2(50). С. 49-67. DOI: https://doi.org/10.37468/2307-1400-2025-2-49-67

Analysis of security threats and information protection measures in computer systems of higher education institutions

Pshenichny Dmitry V. [1]
Dyachenko Yury Y. [1]

[1] *Donetsk National Technical University, Donetsk, Russia*

Abstract
The article conducts an analysis of current cyber threats targeting Russia. The tactics, techniques, and consequences of attacks are examined, and key protective measures for safeguarding information systems against external influences are systematized. The study is based on data from the FSB of Russia, Positive Technologies reports, and other authoritative sources. An algorithm for the cyclic update of protective measures in the information systems of higher educational institutions is proposed.

Keywords: cybersecurity, phishing, malware, social engineering, DDoS attacks, vulnerabilities, data protection, cyber threats, public Wi-Fi networks, information security, multi-level access control, cyclic update of protective measures algorithm.

References

1. Federal Security Service of the Russian Federation. Official statement "The FSB of Russia has recorded more than five thousand hacker attacks on critical infrastructure of the Russian Federation since the beginning of 2022" dated April 13, 2023 [Electronic resource]. – URL: http://www.fsb.ru/fsb/press/message/single.htm!id=10439694@fsbMessage.html (accessed: March 17, 2025).
2. Kaspersky Cyber Threat Intelligence. Cyber threat landscape for Russia and the CIS 2024: analytical report / N. Nazarov, N. Shornikova, V. Burtsev [et al.] – Kaspersky, 2024. – 121 p. [Electronic resource]. – URL: https://www.kaspersky.ru/go/threat-landscape (accessed on April 4, 2025).
3. A Complete Guide to Phishing Attacks // Habr. – 2021. – February 25. [Electronic resource]. – URL: https://habr.com/ru/companies/varonis/articles/544140/ (accessed on March 18, 2025).
4. Phishing Emails: How to Recognize Them and Avoid Becoming Their Victim // Kaspersky. – 2023. – [Electronic resource]. – URL: https://www.kaspersky.ru/resource-center/preemptive-safety/phishing-prevention-tips (accessed on March 19, 2025).
5. Budarny G.S., Dyusmetova A.A., Kazantsev A.A., Krasov A.V. Social engineering: its methods and ways of protection // Actual problems of infotelecommunications in science and education (APINO 2023): Collection of scientific articles. XII International scientific, technical and scientific-methodical conference. In 4 volumes, St. Petersburg, February 28 – January 2, 2023. Volume 1. - St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M.A. Bonch-Bruevich, 2023. - P. 200-204. - EDN PWVWPZ.
6. Matveev D.V. Phishing in the era of digitalization: methods and strategies of protection // Trends in the development of science and education. - 2024. - No. 115-6. - P. 110-115. – DOI 10.18411/trnio-11-2024-262. – EDN MSYLUK.
7. Current Cyber Threats: Q1 2024 // Positive Technologies. – 2024. – May 22 [Electronic resource]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2024-q1/ (date of access: March 21, 2025).
8. Streltsov D. Current Cyber Threats: Q2 2024 // Positive Technologies. – 2024. – August 22 [Electronic resource]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-ii-kvartal-2024-goda/#id2 (date of access: March 21, 2025).
9. Golushko A. Current cyber threats: Q4 2024 – Q1 2025 / A. Golushko // Positive Technologies. – 2025. – March 20 [Electronic resource]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/ (date of access: April 1, 2025).
10. Central Bank of the Russian Federation. Attack 2024: [report] / Bank of Russia. – Moscow, 2024. – 50 p. [Electronic resource]. – URL: https://cbr.ru/Collection/Collection/File/55129/Attack_2024.pdf (date of access: 04.04.2025).
11. Methods for detecting vulnerabilities in security systems // Hanston. – 2024. – February 29. [Electronic resource]. – URL: https://hanston.ru/press-centr/metody-obnaruzheniya-uyazvimostej-v-sistemah-bezopasnosti/ (date of access: 22.03.2025).

12. What is social engineering? // Kaspersky. – 2023. [Electronic resource]. – URL: https://www.kaspersky.ru/resource-center/definitions/what-is-social-engineering (date of access: 23.03.2025).

13. Protodyakonova A.V., Dmitrieva A.N. Information security and the Internet // Current issues of modern science: theory, methodology, practice, innovation: Collection of scientific articles based on the materials of the XIII International scientific and practical conference, Ufa, November 17, 2023. – Ufa: Scientific Publishing Center "Vestnik Nauki", 2023. – Pp. 228-231. – EDN ZKRMYA.

14. Zherokov Z.A., Georgiev I.S. Information security in social networks // Current issues of modern education: Collection of scientific papers. – Kirov: Interregional Center for Innovative Technologies in Education, 2024. – Pp. 78-80. – EDN CKZYJL.

15. Ermakov M.G. "Telephone" fraud // Problems of combating crime in the context of digitalization: theory and practice: Collection of articles from the XVIII International Scientific and Practical Conference, Barnaul, June 29, 2020 / Editors S.I. Davydov, V.V. Polyakov. Volume Issue XVI. – Barnaul: Altai State University, 2020. – Pp. 51-55. – EDN CQTEFK.

16. What are DDoS attacks and how can a telecom operator protect itself from them // VAS Experts. – 2024. – January 11. [Electronic resource]. – URL: https://vasexperts.ru/blog/dpi/chto-takoe-ddos-ataki-i-kak-ot-nih-zashhititsya-operatoru-svyazi/ (date of access: 24.03.2025).

17. Bondarev V.V. Introduction to information security of automated systems: textbook. – 3rd ed. – Moscow: Publishing house of Bauman Moscow State Technical University, 2021. – 252 p.: ill. – ISBN 978-5-7038-5541-6. – EDN BGPOQZ. [Electronic resource]. – URL: https://rucont.ru/efd/808476 (date of access: 04.04.2025).

18. Parshakova M.S., Uspensky N.K. Analysis of threats and risks of using public local wireless Wi-Fi networks // Fundamental and applied scientific research: current issues, achievements and innovations: collection of articles. XXXIX Int. scientific-practical. conf. - Penza: Science and Education, 2020. – Pp. 19-25. – EDN KHQLTA.

19. Skatkov A.V., Bryukhovetsky A.A., Moiseev D.V., Sukharev N.V. Models of distribution of protection resources for mitigating node failures based on the decay vector method under atypical attacks in 5G networks // Bulletin of Tula State University. Technical sciences. - 2023. - No. 7. - Pp. 512-518. – DOI 10.24412/2071-6168-2023-7-512-513. – EDN TKHXXG.

20. Trusilnikov S.V. Organization of a wireless local area network for Tomsk Trunk Company LLC // TUSUR-2009 Scientific Session: Proc. of the All-Russian Scientific and Technical Conf. – Tomsk: V-Spectr, 2008. – Part 2. – Pp. 192–194.

21. Dolgopyatov A.Yu., Dolgopyatov O.A. Software vulnerabilities // Inter-industry studies as a basis for the development of scientific thought: Collection of articles from the International Scientific and Practical Conference in 2 parts, Orenburg, December 27, 2022. Volume Part 1. – Ufa: Limited Liability Company "OMEGA SCIENCES", 2022. – Pp. 60-67. – EDN WKFGBS.

22. Shemsetdinov S. Ya., Dzhanmyradov A., Dovletova G. Ya., Bazarov B. Z. Providing recommendations for strengthening network security // Trends, factors and mechanisms for improving the effectiveness of domestic science: Collection of articles from the National (All-Russian) scientific and practical conference with international participation, Voronezh, September 22, 2024. – Ufa: OOO "Omega Science", 2024. – Pp. 45-47. – EDN KPSQQC.

For citation: Pshenichny D.V., Dyachenko Y.Y. Analysis of security threats and information protection measures in computer systems of higher education institutions // National security and strategic planning. 2025. № 2(50). pp. 49-67. DOI: https://doi.org/10.37468/2307-1400-2025-2-49-67

Сведения об авторах:

Пшеничный Дмитрий Викторович – аспирант кафедры компьютерной инженерии, Донецкий национальный технический университет, г. Донецк, Россия
e-mail: dimon11_22@mail.ru
SPIN-код: 9465-4482

Дьяченко Юрий Юрьевич – аспирант кафедры компьютерной инженерии, Донецкий национальный технический университет, г. Донецк, Россия
e-mail: yury.dja4enko@yandex.ru
SPIN-код: 8644-4750

Information about authors:

Pshenichny Dmitry V. – Postgraduate student of the Computer Engineering Department, Donetsk National Technical University, Donetsk, Russia
e-mail: dimon11_22@mail.ru
SPIN-код: 9465-4482

Dyachenko Yury Y. – Postgraduate student of the Computer Engineering Department, Donetsk National Technical University, Donetsk, Russia
e-mail: yury.dja4enko@yandex.ru
SPIN: 8644-4750