Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ УПРАВЛЕНИЯ»



|  |  |
| --- | --- |
|  | Институт информационных систем |
|  | Кафедра информационных систем |

**Отчет по проектной работе**

|  |  |
| --- | --- |
| **Тема проекта** | Статистическое исследование динамики киберпреступности в |
| контексте актуальной экономической обстановки | |
| *(тема проекта)* | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Направление подготовки** | | | 09.03.03 Прикладная информатика | | | |
| **Образовательная программа** | | | Информационные технологии и системная аналитика | | | |
| **Курс** | **3** | **Группа** | ПИ3-1 |  | **форма обучения** | очная |
|  |  |  |  |  |  |  |
| **Обучающиеся** | | |  |  | Беляев А. Д. | |
| *(подпись)* |  | *(Фамилия и Инициалы)* | |
|  | | |  |  | Нестеров Ф. О. | |
| *(подпись)* |  | *(Фамилия и Инициалы)* | |
|  | | |  |  | Фамилия И.О. | |
| *(подпись)* |  | *(Фамилия и Инициалы)* | |
|  | | |  |  | Фамилия И.О. | |
|  | | | *(подпись)* |  | *(Фамилия и Инициалы)* | |
|  | | |  |  | Фамилия И.О. | |
|  | | | *(подпись)* |  | *(Фамилия и Инициалы)* | |
| **Куратор проекта** | | |  |  | Белоусова М. Н. | |
|  | | | *(подпись)* |  | *(ученая степень, звание, Фамилия и Инициалы)* | |
| **Дата сдачи проекта** | | | |  | 02 мая 2024 г. | |

**Москва – 2025**

**Список исполнителей**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | ФИО (полностью) обучающегося | Дата защиты | Оценка | Подпись руководителя |
|  | Беляев Антон Дмитриевич | 02.05.2025 |  |  |
|  | Нестеров Филипп Олегович | 02.05.2025 |  |  |

**Оглавление**

[**Введение** 4](#_Toc197014507)

[**1** **Стейкхолдеры и обоснование актуальности проекта** 6](#_Toc197014508)

[**2** **Результат проделанной работы** 9](#_Toc197014509)

[**3** **Планирование и распределение задач по проекту** 24](#_Toc197014510)

[**Заключение** 27](#_Toc197014511)

[**Список использованных источников** 29](#_Toc197014512)

# **Введение**

Проект "Исследование изменений в сфере киберпреступности в условиях современных экономических реалий" направлен на анализ текущих тенденций цифровой преступности, изучение ее взаимосвязи с экономическими процессами и разработку прогнозов дальнейшего развития. Активное внедрение цифровых технологий, сопровождающееся увеличением количества данных и онлайн-транзакций, создает новые уязвимости, которые используются преступниками. В периоды экономической нестабильности, когда организации и государственные структуры вынуждены оптимизировать расходы, вопросы кибербезопасности приобретают особую значимость.

Актуальность проекта определяется тем, что современная киберпреступность представляет собой серьезную угрозу не только для информационной инфраструктуры, но и для экономики в целом. Анализ динамики кибератак позволяет выявить основные закономерности их развития и разработать эффективные меры защиты для бизнеса, частных пользователей и государственных институтов. Особое внимание уделяется исследованию влияния экономических кризисов на трансформацию методов киберпреступности, что приводит к усложнению атак и увеличению их количества.

Цель проекта заключается в проведении статистического анализа динамики киберпреступности, выявлении взаимосвязи между экономическими изменениями и ростом киберугроз, а также построении оптимистичных и пессимистичных прогнозов. Полученные результаты могут служить основой для разработки адаптированных мер кибербезопасности в условиях экономической нестабильности.

Проект включает исследование влияния экономических кризисов на динамику киберпреступности, анализ ключевых статистических данных и выработку рекомендаций для повышения уровня информационной безопасности. Использование методов математической статистики, таких как анализ относительных, абсолютных и средних величин, а также методов прогнозирования на основе скользящей средней, позволило выявить закономерности в развитии киберугроз. Результаты исследования представлены в наглядной форме с использованием графиков и таблиц.

Новизна исследования заключается в применении междисциплинарного подхода, сочетающего методы статистического анализа с экономическими моделями. Это позволяет не только изучать исторические тенденции киберпреступности, но и прогнозировать ее развитие с учетом влияния экономических факторов, таких как финансовые кризисы и периоды нестабильности.

Проект представляет собой научное исследование, соответствующее направлениям подготовки в сфере информационной безопасности, прикладной информатике и статистики. Результаты работы могут быть использованы студентами, специалистами по кибербезопасности, а также представителями бизнеса и государственных органов. Практическая ценность исследования состоит в возможности прогнозирования киберугроз и разработке адаптивных систем защиты, учитывающих изменения экономической ситуации.

Ожидается, что исследование позволит:

1. Выявить ключевые тенденции в развитии киберпреступности.
2. Сформулировать оптимистичные и пессимистичные прогнозы, которые помогут эффективно планировать ресурсы и меры противодействия кибератакам.

Данный проект предоставляет инструменты для повышения уровня киберзащиты в условиях нестабильной экономической обстановки, что особенно важно в современном цифровом мире.

# **Стейкхолдеры и обоснование актуальности проекта**

Описание заинтересованных сторон

1. Государственный университет управления (ГУУ)  
    ГУУ является одним из ведущих научно-учебных комплексов в стране, активно поддерживающим развитие управленческого образования и научных исследований.
2. Заинтересованность:

Научная репутация: публикации студентов способствуют формированию положительного имиджа университета как авторитетного научного учреждения. Это повышает его рейтинг среди университетов и делает его более привлекательным для абитуриентов и партнеров.

Поддержка научных проектов: успешные студенческие публикации демонстрируют эффективность финансируемых университетом исследовательских проектов, что способствует привлечению дополнительного финансирования на научную деятельность.

1. Методы взаимодействия:

Обеспечение студентам доступа к научным базам данных, инструментам анализа и экспертной поддержке.

Организация семинаров и научных конференций для представления результатов исследований.

Оценка качества научных работ и предоставление обратной связи.

1. Студенты, проходящие обучение в ГУУ Студенты, участвующие в написании статьи, развивают свои академические и исследовательские навыки, а также получают возможность представить свои результаты широкой аудитории.
2. Заинтересованность:

Академическое развитие: участие в проекте помогает студентам укрепить аналитические и критические навыки, освоить методы работы с данными и получить практический опыт написания научных статей. Это способствует лучшему усвоению образовательной программы.

Участие в научном сообществе: публикации дают студентам возможность представить свои исследования на конференциях, получить признание среди экспертов и интегрироваться в профессиональное научное сообщество.

1. Методы взаимодействия:

Консультирование со стороны преподавателей и экспертов.

Возможность публикации результатов исследований в научных журналах и презентации их на профильных мероприятиях.

Предоставление платформы для коллективного обсуждения идей и получения рекомендаций.

Обоснование актуальности проекта

Проект «Статистическое исследование динамики киберпреступности в контексте актуальной экономической обстановки» обладает высокой актуальностью в условиях современной цифровой трансформации.

Для университета:

Участие студентов в проекте повышает научную активность и репутацию ГУУ. Это привлекает внимание к вузу как к ведущему научному центру, а также демонстрирует его способность адаптироваться к современным вызовам, включая вопросы информационной безопасности.

Для студентов:

Проект предоставляет возможность изучить важную и современную тему, получить опыт в использовании методов статистики и анализа данных, а также развить навыки академического письма. Это способствует не только их профессиональному, но и личностному росту.

Для общества и бизнеса:

Полученные результаты помогут лучше понять динамику киберугроз и разработать эффективные меры защиты в условиях экономической нестабильности. Это особенно важно для компаний, пользователей и государственных структур, которые сталкиваются с растущими рисками в цифровом пространстве.

Почему решение поможет:

Для университета: проект укрепит его научный авторитет.

Для студентов: участие в исследовании повысит их конкурентоспособность на рынке труда.

Для общества: представленные данные и прогнозы помогут принять меры для повышения кибербезопасности.

Таким образом, проект одновременно решает задачи образовательного, научного и прикладного характера, что делает его полезным для всех ключевых стейкхолдеров.

# **Результат проделанной работы**

  Сегодня информация играет ключевую роль в любой деятельности. Технологии современности предоставляют возможности для быстрой передачи и гибкой обработки данных. Однако эти же технологии способствуют росту киберпреступности. Основные виды киберпреступлений включают фишинг, распространение вредоносных программ, хищение информации и DoS-атаки.

Многие ученые Российской Федерации занимались вопросами кибербезопасности. Так, А. В. Шободоевой и Е. А. Муньковой в своих научных трудах исследовали проблемы информационной безопасности [1], а Д. А. Тершуков обосновал важность информационной безопасности как составной части национальной безопасности страны [2]. Вопросы реализации противодействия преступлений в киберпространстве были рассмотрены отечественными учеными Н. А. Казаковой, А. А. Петюковой [3], Б. А. Тарчоковым [4], Т. А. Гончаровой и Л. В. Набоковым [5].

Был проведен анализ статистических данных о преступлениях, которые были совершены в области компьютерной информации в Российской Федерации или с использованием информационно-телекоммуникационных технологий [6; 7; 8].

 Основные результаты анализа:

 Согласно данным за 2022–2024 годы, общее число зарегистрированных киберпреступлений существенно выросло. В 2022 году было зарегистрировано 522,1 тыс. преступлений (+0,8% к предыдущему году), в 2023 году — 677,0 тыс. (+29,7%), а в январе-августе 2024 года — 500,4 тыс. (+16,4%).

 Наибольшее количество преступлений связано с использованием Интернета и мобильной связи. В 2024 году 83,4% киберпреступлений совершено с использованием Интернета, а 46,3% — с применением мобильных устройств.

 Прогнозы и визуализация данных:

 Для построения прогнозов использовался метод скользящей средней. Этот метод позволяет выделить общую тенденцию в данных и устранить случайные колебания, что особенно важно при анализе динамических рядов. Скользящая средняя рассчитывается путем усреднения значений за определенный период времени. Такой подход дает возможность спрогнозировать будущие значения, основываясь на исторических данных. На основе этого метода были построены графики изменения количества киберпреступлений, которые продемонстрировали устойчивый рост числа инцидентов.

 Скользящая средняя помогла выявить долгосрочные тренды, такие как рост мошеннических операций с использованием Интернета и мобильных устройств, а также сокращение числа атак с использованием вредоносного ПО.

Было проведено исследование развития угроз в информационных сферах по кварталам, за период I квартал 2023 – III квартал 2024 г [9; 10; 11].

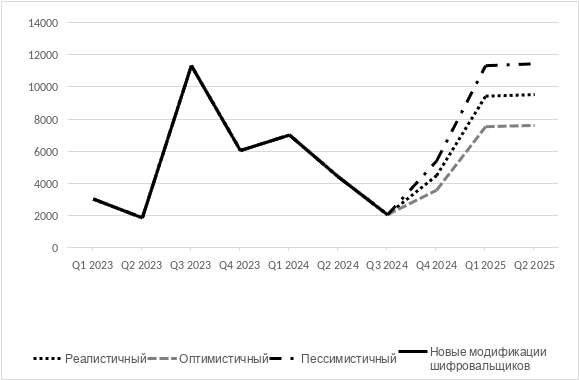


Рисунок 1 – Динамика новых модификаций шифрования

График демонстрирует динамику появления новых версий программ-шифровальщиков. Пик активности приходится на середину 2023 года, что может быть связано с распространением программ-вымогателей через фишинговые кампании и уязвимости в системах пользователей.

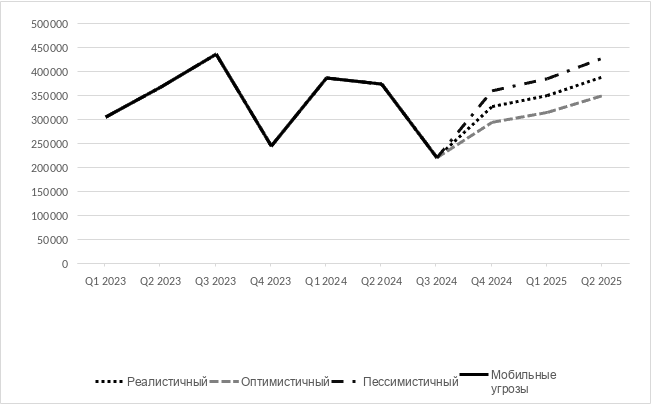


 Рисунок 2 – Динамика мобильных угроз

Данный график показывает количество различных мобильных нарушений безопасности за период с 2023 по 2025 годы, предполагаемый реалистичный прогноз указывает, что число мобильных атак не снизится и будет приравнено к показателям за первую четверть 2024 года.

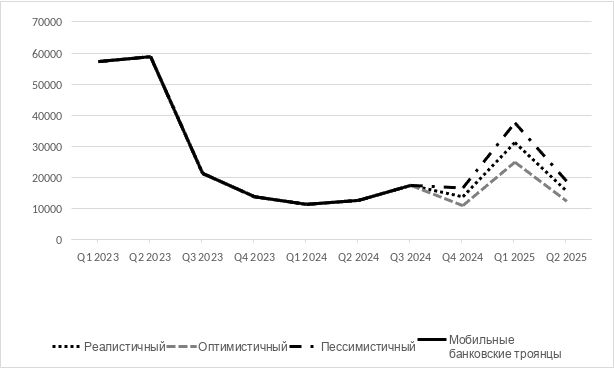


 Рисунок 3 – Динамика Мобильных банковских троянцев

Этот график отображает рост числа обнаруженных мобильных банковских троянцев. За период исследования количество таких пакетов ослабло, что указывает на уменьшение успешных атак, направленных на кражу финансовых данных пользователей мобильных приложений.

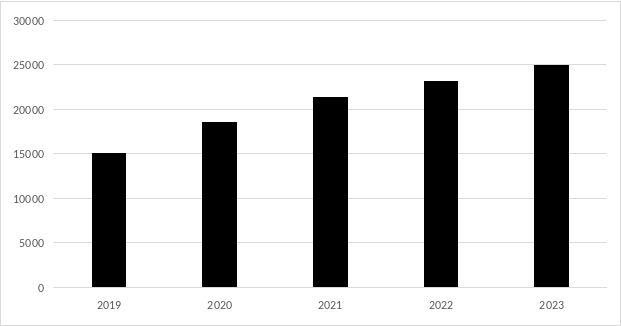


Рисунок 4 - Динамика новых уязвимостей (CVE)

График показывает количество новых уязвимостей (CVE), зарегистрированных в период с 2019 по 2023 годы. Число CVE растет ежегодно, что свидетельствует об увеличении числа выявленных уязвимостей в программном обеспечении и необходимости регулярных обновлений для предотвращения атак.



 Рисунок 5 – График динамики разных типов кибератак по кварталам

График показывает динамику роста различных типов информационных угроз по кварталам. На графике видно, что с каждым кварталом количество инцидентов, связанных с киберугрозами, стабильно увеличивается. Это подтверждает рост активности киберпреступников и необходимость принятия превентивных мер кибербезопасности.

 В ходе исследования были выявлены несколько ключевых уязвимостей, активно используемых киберпреступниками.

По данным Kasperky Secure Network, после предоставления компанией OpenAI публичного доступа к GPT-3 в конце 2022 года, злоумышленники использовали её для создания персонализированных убедительных писем для целевого фишинга. К тому же, данная языковая модель использовалась для генерации последующих реплик после получения ответа от получателя фишингового сообщения. Была обнаружена вредоносная компания, которая эксплуатировала приобретающую популярность ChatGPT, которая заключалась в предоставлении фальшивых данных для доступа к платной версии языковой модели с правдоподобной ссылкой на скачивание поддельной версии ChatGPT для Windows. По ссылке на устройство загружался троянец, который воровал учетные данные из многих популярных браузеров [12].

Были обнаружены в магазине Google Play вредоносные приложения, которые маскируются под модифицированные версии Telegram на уйгурском, традиционном и упрощённом китайском языках. Описания для данных приложений содержали схожие иллюстрации приложения с официальной страницы Telegram в магазине. В коде приложений был обнаружен шпионский модуль, задачей которого являлась постоянная слежка за работой приложения и отправка данных на сервер злоумышленников: контакты, сообщения, названия чатов, имя и телефон учетной записи [13].

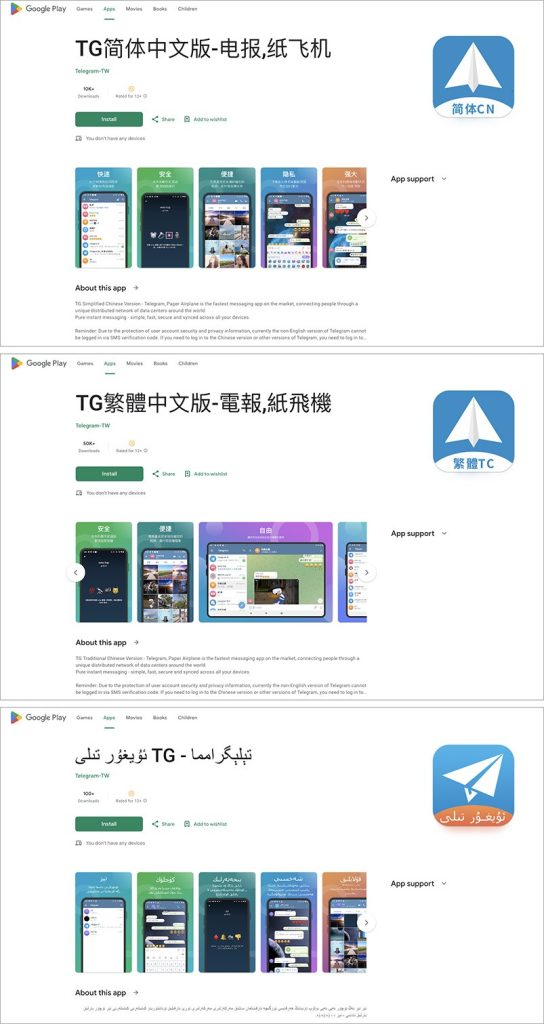


Рисунок 6 – Иллюстрации приложений в магазине Google Play

В рассылке от Openwall Oopen Source Security было заявлено об обнаружении бэкдора в XZ, которая встроена во многие популярные дистрибутивы Linux. Для доступа к функциям systemd на таких дистрибутивах, как Debian, Ubuntu и Fedora, использовался модифицированный OpenSSH, который зависел от этой библиотеки. Вредоносный код был внедрён в феврале и марте 2024 года. Полагается, что целью атаки являлось в добавление sshd возможности удаленного выполнения кода [14].

Эти уязвимости демонстрируют необходимость усиления мер кибербезопасности и постоянного мониторинга угроз, чтобы минимизировать риски утечек данных и взломов систем.

Статистика по наиболее активным вымогательским группам опирается на количество жертв, добавленных злоумышленниками на сайты DLS (data leak site) за отчетный период. В третьем квартале наиболее активной была группа RansomHub, жертвы которой составили 17,75% от общего числа.

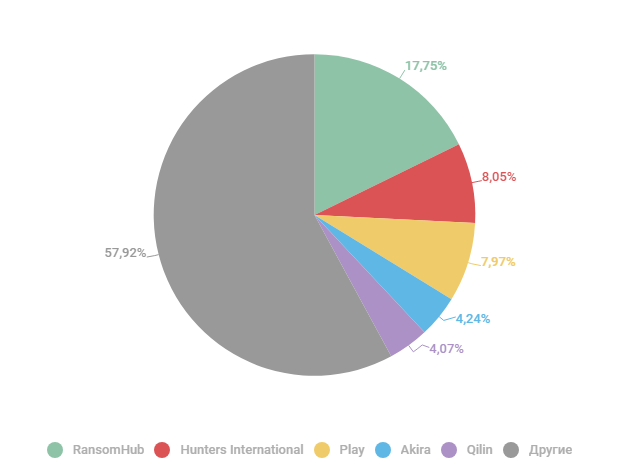


Рисунок 6 - Доля жертв конкретной группы (по данным ее сайта DLS) среди всех жертв всех групп, опубликованных на всех рассмотренных сайтах DLS за отчетный период

Была выявлена продолжительная кампанию по краже криптовалюты, жертвами которой стали более 15 000 пользователей в 52 странах. Злоумышленники использовали метод, известный более десяти лет: изначально он применялся в банковских троянцах для подмены номеров банковских счетов. Однако в последней кампании злоумышленники заражали устройства жертв с помощью троянизированной версии браузера Tor. Цепочка заражения выглядела так: жертва загружает со стороннего ресурса троянизированный установщик Tor, который содержит защищенный паролем RAR-архив, — пароль помогает избежать обнаружения защитными решениями. После проникновения в целевую систему вредоносный файл прописывается в автозагрузке и использует для маскировки значок популярного приложения, например uTorrent.

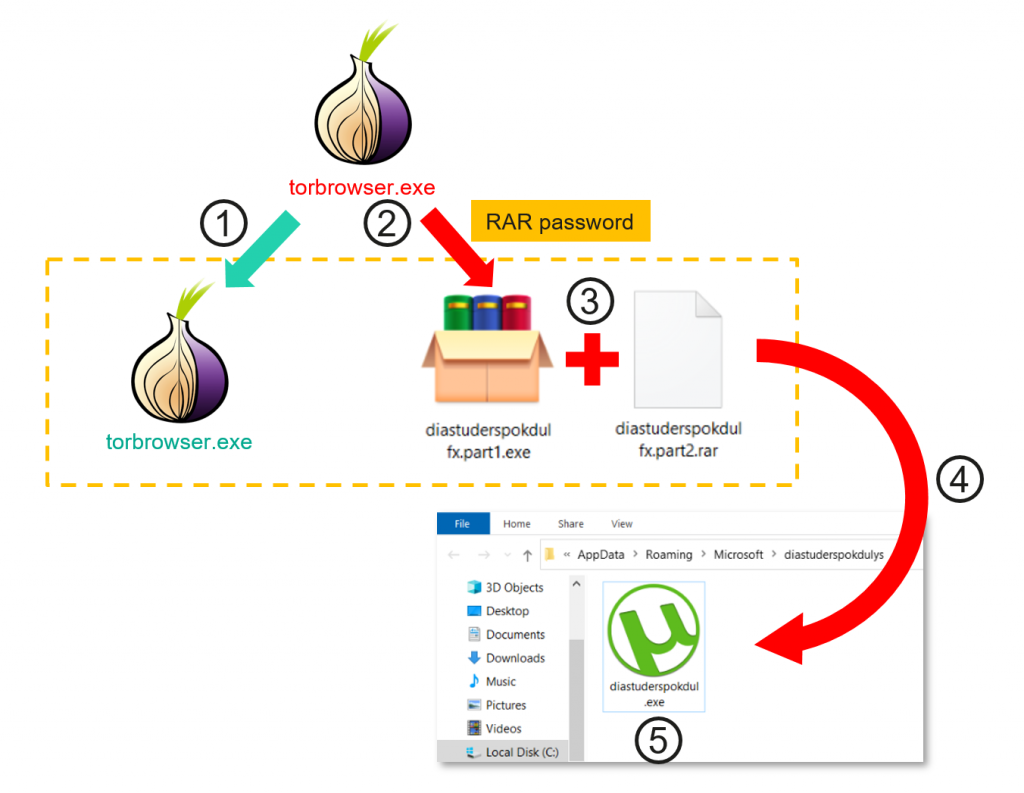


Рисунок 7 – цепочка заражения системы путем маскировки под uTorrent

Зловред отслеживает содержимое буфера обмена — если текст содержит адрес криптовалютного кошелька, он заменяет его на адрес кошелька злоумышленников.

Было проведено исследование при помощи тестирования 16 различных антивирусов. В состав тестируемых антивирусов входят:   
Avast Free Antivirus 24.8, [AVG Internet Security 24.7](https://www.av-comparatives.org/vendors/avg/), [Avira Free Security 1.1](https://www.av-comparatives.org/vendors/avira/), [Bitdefender Total Security 27.0](https://www.av-comparatives.org/vendors/bitdefender/), [ESET HOME Security Essential 17.2](https://www.av-comparatives.org/vendors/eset/), [F-Secure Internet Security 19.5](https://www.av-comparatives.org/vendors/f-secure/), [G DATA Total Security 25.5](https://www.av-comparatives.org/vendors/g-data/), [Kaspersky Standard 21.18](https://www.av-comparatives.org/vendors/kaspersky-lab/), [McAfee Total Protection 1.21](https://www.av-comparatives.org/vendors/mcafee/), Microsoft Defender Antivirus 4.18, Norton Antivirus Plus 22.24, Panda Free Antivirus 22.02, Quick Heal Internet Security 24.0, Total Defense Essential Anti-Virus 14.0, TotalAV Antivirus Pro 6.0, Trend Micro Internet Security 17.8 (цифры указывают используемую версию при тестировании)

Ниже предоставлены графики про анализируемых антивирусов и их работоспособность за разные временные промежутки.

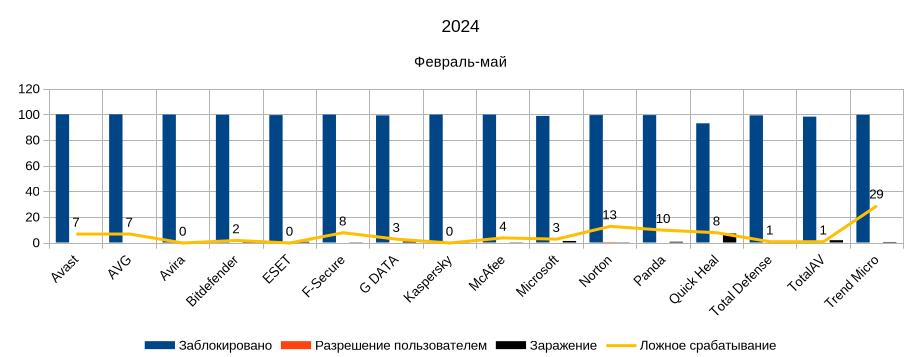


Рисунок 8 – тестирование антивирусов февраль-май

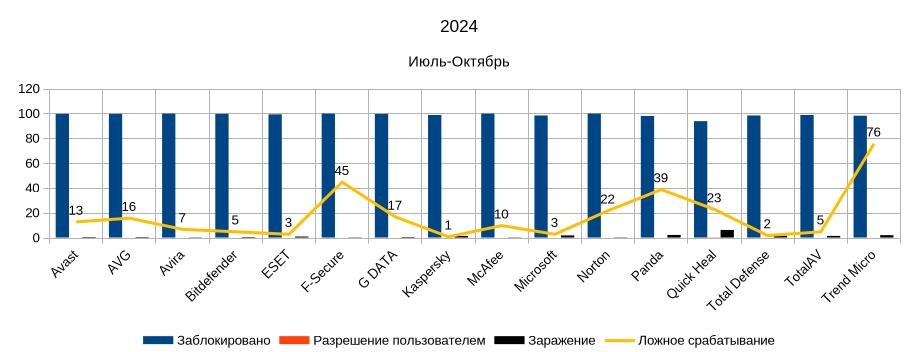


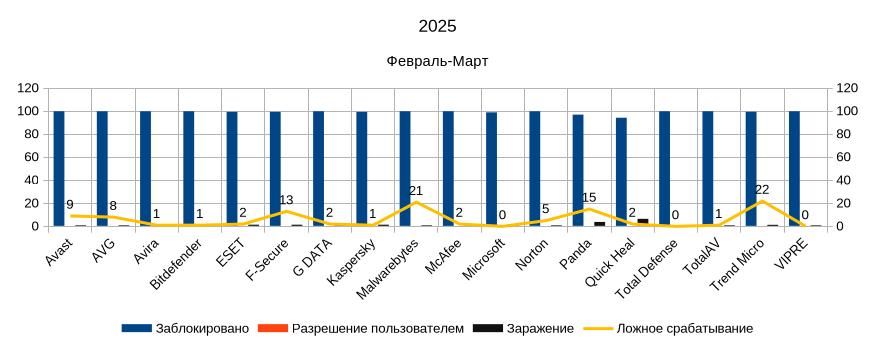
Рисунок 9 – тестирование антивирусов июль-октябрь 

Рисунок 10 – тестирование антивирусовфевраль-март

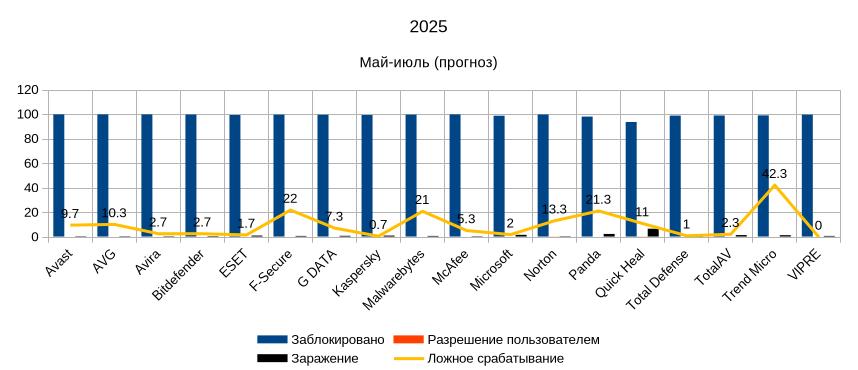


Рисунок 11 – тестирование антивирусов май-июль (прогноз)

1. Эффективность блокировки угроз (Blocked): Большинство антивирусов демонстрируют высокую эффективность (более 99%) в блокировке угроз. Исключение — "Quick Heal" с показателем около 93-94%. В прогнозируемых данных на 2025 год наблюдается небольшое снижение эффективности у некоторых вендоров (например, у Panda — 97.9%, у Microsoft — 98.6%).

2. Пропущенные угрозы (Compromised): Наименьший процент пропущенных угроз у Avira, F-Secure, McAfee (0.2% или ниже). Наибольший процент у "Quick Heal" (6-7%), Panda (2.1-3.4%) и Microsoft (1.2-1.7%). В прогнозе на 2025 год у некоторых антивирусов (например, Panda) прогнозируется увеличение пропущенных угроз.

3. Ложные срабатывания (FPs): Наименьшее количество ложных срабатываний у Avira, Kaspersky, Microsoft (0-3). Наибольшее количество у "Trend Micro" (22-76), F-Secure (8-45) и Norton (13-22). В прогнозе на 2025 год у "Trend Micro" ожидается снижение FPs с 76 до 42.3, но это все равно высокий показатель.

4. Динамика изменений: у некоторых антивирусов (например, Kaspersky, Microsoft) наблюдается улучшение показателей со временем (снижение пропущенных угроз и ложных срабатываний).

Panda и "Quick Heal" стабильно демонстрируют более низкую эффективность по сравнению с другими. В прогнозируемых данных появляются новые вендоры (Malwarebytes, VIPRE), которые показывают хорошие результаты.

5. Особенности данных: Показатель "User dependent" почти всегда равен 0, за исключением "Quick Heal" (0.2%) и Norton (0.4% в одном из периодов). Это может указывать на то, что большинство угроз блокируются автоматически. Разброс значений FPs у некоторых вендоров (например, "Trend Micro") может быть связан с изменениями в алгоритмах детектирования или тестовых выборках.

В рамках анализа было проведено дополнительное исследование другого типа тестирование. Ниже представлен обзор проведенного анализа и краткая информация о результатах тестирования.

В данном случае были протестированы пять популярных антивирусных решений: Avast, Kaspersky, Eset, Bitdefender и Microsoft Defender.

1. Avast

|  |
| --- |
| Защита (Protection Score): 6.9 / 8.0 |
| Защита от 0-day атак: 601 образец использован. Avast показал высокую эффективность в блокировании новых угроз. |
| Обнаружение распространенного вредоносного ПО: 15,629 образцов. Продукт успешно идентифицировал большинство угроз. |
| Производительность (Performance Score): 6.9 / 8.0 |
| Замедление работы системы при посещении веб-сайтов: 21%. |
| Замедление загрузки приложений: 5%. |
| Удобство использования (Usability Score): 6.9 / 8.0 |
| Ложные срабатывания при посещении веб-сайтов: 0. |
| Ложные обнаружения легитимного ПО: 1. |

Таблица 1 – результаты Avast

2. Kaspersky

|  |
| --- |
| Защита (Protection Score): 8.0 / 8.0 |
| Защита от 0-day атак: 601 образец. Kaspersky продемонстрировал 100% эффективность. |
| Обнаружение распространенного вредоносного ПО: 15,629 образцов. Все угрозы были успешно обнаружены. |
| Производительность (Performance Score): 7.5 / 8.0 |
| Замедление работы системы: 15%. |
| Замедление загрузки приложений: 2%. |
| Удобство использования (Usability Score): 7.8 / 8.0 |
| Ложные срабатывания при посещении веб-сайтов: 0. |
| Ложные срабатывания: 0. |

Таблица 2 – результаты Kaspersky

1. Eset

|  |
| --- |
| Защита (Protection Score): 7.2 / 8.0 |
| Защита от 0-day атак: 601 образец. Eset показал хорошие результаты, но уступил Kaspersky. |
| Обнаружение распространенного вредоносного ПО: 15,629 образцов. |
| Производительность (Performance Score): 7.0 / 8.0 |
| Замедление работы системы: 18%. |
| Замедление загрузки приложений: 2%. |
| Удобство использования (Usability Score): 7.5 / 8.0 |
| Ложные срабатывания при посещении веб-сайтов: 0. |
| Ложные срабатывания: 1. |

Таблица 3 – результаты East

1. Bitdefender

|  |
| --- |
| Защита (Protection Score): 7.8 / 8.0 |
| Защита от 0-day атак: 601 образец. Bitdefender близок к Kaspersky по эффективности. |
| Обнаружение распространенного вредоносного ПО: 15,629 образцов. |
| Производительность (Performance Score): 7.2 / 8.0 |
| Замедление работы системы: 16%. |
| Замедление загрузки приложений: 2%. |
| Удобство использования (Usability Score): 7.6 / 8.0 |
| Ложные срабатывания при посещении веб-сайтов: 0. |
| Ложные срабатывания: 0. |

Таблица 4 – результаты Bitdefender

1. Microsoft Defender

|  |
| --- |
| Защита (Protection Score): 7.2 / 8.0 |
| Защита от 0-day атак: 601 образец. Microsoft Defender показал средние результаты. |
| Обнаружение распространенного вредоносного ПО: 15,629 образцов. |
| Производительность (Performance Score): 6.8 / 8.0 |
| Замедление работы системы: 20%. |
| Замедление загрузки приложений: 2%. |
| Удобство использования (Usability Score): 6.9 / 8.0 |
| Ложные срабатывания при посещении веб-сайтов: 0. |
| Ложные срабатывания: 2. |

Таблица 5 – результаты Microsoft Defender

Методы тестирования антивирусов

Test Modules under Windows Protection

Тестирование антивирусных продуктов проводится в условиях, максимально приближенных к реальным угрозам. Основные этапы тестирования включают:

Stage 1 – Test of the protection function: защита от 0-day атак Цель: Проверить способность продукта блокировать новейшие угрозы, включая веб-атаки и угрозы через электронную почту. Процедура: Продукты устанавливаются с настройками по умолчанию. Система заражается через вредоносные веб-сайты или письма. Фиксируются все попытки блокировки угроз, включая: Блокировку URL. Обнаружение и блокировку эксплойтов. Предотвращение загрузки вредоносных компонентов. Успешность блокировки проверяется мониторингом системы.

Stage 2 – Test of the detection function: обнаружение распространенного вредоносного ПО Цель: проверить способность продукта обнаруживать известные угрозы, которые могут присутствовать в сети или на ПК. Процедура: проводится сканирование системы с использованием эталонного набора вредоносных программ (AV-TEST reference set). Все необнаруженные файлы запускаются для проверки динамического обнаружения.

Условия тестирования: Все продукты тестируются одновременно на идентично настроенных системах. Продукты имеют полный доступ к Интернету и регулярно обновляются.

Тестирование показало, что Kaspersky и Bitdefender демонстрируют наивысшую эффективность в защите от 0-day атак и обнаружении распространенного вредоносного ПО. Avast и Eset также показали хорошие результаты, в то время как Microsoft Defender уступил конкурентам. Методы тестирования AV-TEST обеспечивают объективную оценку защитных возможностей антивирусов в условиях, приближенных к реальным угрозам.

# **Планирование и распределение задач по проекту**

Целью проекта является написание научной статьи на тему: "Статистическое исследование динамики киберпреступности в контексте актуальной экономической обстановки". Для достижения этой цели проект был разбит на несколько этапов с четко определенными задачами, сроками, ответственными участниками, средствами реализации и ожидаемыми результатами.

Первым шагом стало исследование темы. В течение первых двух недель Нестеров Филипп Олегович собирал и анализировал информацию из книг, научных статей и интернет-ресурсов. На этом этапе удалось глубже понять основные аспекты темы и сформулировать ключевые аргументы для будущей статьи.

После завершения анализа информации была создана структура статьи. Беляев Антон Дмитриевич разработал план, включающий введение, основную часть и заключение. Этот процесс занял одну неделю и позволил четко определить направление дальнейшей работы.

Третий этап заключался в написании черновика текста статьи. В течение месяца Нестеров Филипп Олегович подготовил черновые версии введения, основной части и заключения. В работе использовались текстовые редакторы, такие как Word, а также платформы для совместной работы, например, Gitflic.

После написания черновика начался этап редактирования и коррекции текста. Беляев Антон Дмитриевич в течение месяца работал над улучшением структуры и стиля, исправляя грамматические ошибки и логические недочеты. Это помогло сделать статью более ясной и профессиональной.

Особое внимание было уделено визуализации данных. В течение двух недель оба участника проекта занимались созданием графиков, таблиц и схем с помощью Excel, PowerPoint и специализированных аналитических инструментов. Эти материалы стали важной частью статьи, наглядно демонстрируя основные выводы исследования.

Заключительным этапом стала подготовка презентации результатов. В течение недели Нестеров Филипп Олегович подготовил презентацию, которая обобщила все ключевые аспекты работы.

Одной из сильных сторон проекта стала креативность участников и способность генерировать оригинальные идеи. Эти качества позволили глубже изучить тему и предложить нестандартные подходы. Кроме того, понимание потребностей аудитории и адаптация материала под их интересы также сыграли положительную роль. Однако слабым местом оказалось недостаточное использование обратной связи, что могло повлиять на скорость работы и качество текста.

Среди внешних факторов основными угрозами стали конкуренция и технические проблемы. Наличие аналогичных публикаций от других авторов могло снизить уникальность проекта, а возможные сбои в программном обеспечении создавали риски для своевременного завершения работы. В то же время возможности для проекта включали доступ к актуальным данным и методам анализа, а также поддержку со стороны научного сообщества и университета, что могло повысить шансы на публикацию статьи.

Четкое планирование задач, распределение ролей и учет факторов, влияющих на проект, обеспечили эффективную работу над исследованием. Ожидается, что результаты статьи не только будут опубликованы, но и принесут пользу научному сообществу, подчеркивая важность анализа динамики киберпреступности в условиях современной экономической обстановки.

# **Заключение**

В рамках данного проекта была достигнута его основная цель — проведен статистический анализ динамики киберпреступности с учетом влияния экономических изменений. Были выявлены ключевые взаимосвязи между экономической нестабильностью и ростом киберугроз, что позволило построить оптимистичные и пессимистичные прогнозы.

На основе анализа данных за последние годы была подтверждена устойчивая тенденция к увеличению числа киберпреступлений, особенно связанных с использованием интернета и мобильных устройств. Использование метод скользящей средней, позволило устранить случайные колебания в данных и выделить долгосрочные тренды. Были выявлены ключевые уязвимости, такие как фишинговые атаки, вредоносные приложения и злоупотребление современными языковыми моделями.

Проект также продемонстрировал важность учета экономических факторов при разработке мер кибербезопасности. Финансовые кризисы и экономическая нестабильность создают условия для появления новых форм кибератак, что требует адаптации существующих защитных механизмов. Предложенные в проекте прогнозы могут служить основой для создания эффективных стратегий противодействия киберпреступности.

Полученные результаты подтверждают необходимость усиления мониторинга и проактивного подхода к вопросам кибербезопасности. Они могут быть полезны для государственных структур, коммерческих организаций и индивидуальных пользователей при разработке и внедрении адаптированных мер защиты.

Проект внес вклад в развитие научного потенциала его участников. Выполнение задач способствовало развитию навыков анализа данных, написания научных текстов, а также повышению компетенций в области информационной безопасности. В завершение можно отметить, что исследование создало основу для дальнейших научных работ в области изучения взаимосвязи между экономикой и киберпреступностью, что имеет высокую практическую значимость в современном цифровом мире.

# **Список использованных источников**

1. Шободоева А. В., Мунькова Е. А. Угрозы информационной безопасности Российской Федерации // Проблемы обеспечения национальной безопасности в контексте изменения геополитической ситуации. Иркутск, 2017. С. 244—254. ПРОБЛЕМЫ РАЗВИТИЯ ЭКОНОМИКИ И УПРАВЛЕНИЯ 48

2. Тершуков Д. А. Анализ современных угроз информационной безопасности // NBI-technologies. 2018. № 3. URL: https://cyberleninka.ru/article/n/analiz-sovremennyh-ugroz-informatsionnoy-bezopasnosti (дата обращения: 14.05.2022).

3. Казакова Н. А., Петюкова А. А. Анализ развития рынка кибербезопасности в России и за рубежом // Маркетинг в России и за рубежом. 2021. № 1. С. 57—64.

4. Тарчоков Б. А. Тенденции развития киберпреступности в глобальном информационном пространстве // Проблемы экономики и юридической практики. 2021. Т. 17, № 1. С. 198—201.

5. Гончарова Т. А., Набоков Л. В. Киберпреступность в России: проблемные аспекты и предупреждение преступности // Инновационная экономика и право. 2022. № 1. С. 118—124.

6. Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2022 года. URL: https://мвд.рф/reports/item/35396677/ (дата обращения: 20.12.2024).

7. Краткая характеристика состояния преступности в Российской Федерации за январь-декабрь 2023 года. URL: https://мвд.рф/reports/item/55225633 (иедата обращения: 20.12.2024).

8. Краткая характеристика состояния преступности в Российской Федерации за январь-август 2024 года. URL: https://мвд.рф/reports/item/47055751/ (дата обращения: 20.12.2024).

9. Данные Kaspersky Security Network. URL: <https://securelist.ru/it-threat-evolution-q1-2024-mobile-statistics/109636/> (дата обращения: 21.12.2024)

10. Данные Kaspersky Security Network. URL: <https://securelist.ru/it-threat-evolution-q2-2024-mobile-statistics/110420/> (дата обращения: 21.12.2024)

11. Данные Kaspersky Security Network. URL: <https://securelist.ru/malware-report-q3-2024-mobile-statistics/111143/> (дата обращения: 24.12.2024)

12. Развитие информационных угроз в первом квартале 2023 года. URL: <https://securelist.ru/it-threat-evolution-q1-2023/107467/> (дата обращения: 24.12.2024)

13. Развитие информационных угроз в третьем квартале 2023 года. URL: https://securelist.ru/it-threat-evolution-q3-2023/108446/ (дата обращения: 25.12.2024)

14. Развитие информационных угроз во втором квартале 2024 года. URL: <https://securelist.ru/it-threat-evolution-q2-2024/110409/> (дата обращения: 25.12.2024)

**ПРИЛОЖЕНИЕ 1. Сведения о проекте BusinessChain**

|  |  |
| --- | --- |
| **Номер проекта:** | 2024-1966 |
| **Название трека** | *От идеи к реализации* |
| **Результат выполнения:** | *Полностью* |
| **Ссылка на страницу проекта в БЧ** | *https://businesschain.io/details/project-details?id=18770* |

|  |
| --- |
|  |
| *(подпись куратора с расшифровкой)* |

|  |
| --- |
| **Снимок экрана (скриншот), подтверждающий выполнение этапов трека:** |
|  |
| **Снимок экрана (скриншот), отзыва куратора проектной команды на Businesschain (последний этап трека):** |
|  |

**ПРИЛОЖЕНИЕ 2. Сведения о посещённых Мероприятиях проектного дня**

2.1 Беляев А. Д.

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование мероприятия** | **Ссылка на мероприятие в Makeevents** |
| **1** | *Геймдев: реализ. проектов с применением гейм-технологий* | *https://guu.make.events/eventsNew/q0jtLr* |
| **2** | *Система управления разработкой проекта* | *https://guu.make.events/eventsNew/cI9rLv* |
| **3** | *Личная стратегия, как необходимый ключ к успеху* | *https://guu.make.events/eventsNew/JPT8t3* |
| **4** | *Знакомство с произв. ПО и ИИ с интеракт. участием зала* | *https://guu.make.events/eventsNew/a0LAUk* |
| **5** | *Математические методы в управлении* | *https://guu.make.events/eventsNew/c1s7Kk* |
| **6** | *Написание научной статьи исследовательского характера* | *https://guu.make.events/eventsNew/v9Owcp* |
| **7** | *Как построить успешную карьеру в крупной компании* | *https://guu.make.events/eventsNew/vOv8hp* |

|  |  |
| --- | --- |
| **Ссылка на профиль студента Makeevents** | *https://make.events/public/user/OzTphr* |

|  |
| --- |
| Снимок экрана (скриншот), подтверждающий посещение мероприятия |
|  |

2.2 Нестеров Ф. О.

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование мероприятия** | | **Ссылка на мероприятие в Makeevents** |
| **1** | *Роботизация и искусственный интеллект в HR* | | *https://guu.make.events/eventsNew/qds7zk* |
| **2** | *НЕФТЕГАЗ-2025* | | *https://guu.make.events/eventsNew/C8Oghv* |
| **3** | *Эволюция денежного инструмента.Цифровой рубль.* | | *https://guu.make.events/eventsNew/YIOt9r* |
| **4** | *"Предзащита" проектов проектного обучения для 3 курса* | | *https://guu.make.events/eventsNew/J0sgw3* |
| **5** | *Тестирование универсальных компетенций* | | *https://guu.make.events/eventsNew/KP9wtk* |
| **6** | *Клуб развития международного бизнеса и туризма* | | *https://guu.make.events/eventsNew/C9LFzl* |
| **7** | *Клуб "Школа молодого психолога"* | | *https://guu.make.events/eventsNew/YPh8cD* |
| **8** | *Клуб "Школа молодого психолога"* | | *https://guu.make.events/eventsNew/qPjgzr* |
| **9** | *Маркетинг впечатлений: как очARовать потребителя* | | *https://guu.make.events/eventsNew/JIvwcWё* |
| **10** | *Мастер-класс «Идеи для создания устойчивых проектов»* | | *https://guu.make.events/eventsNew/vO9mUp* |
| **Ссылка на профиль студента Makeevents** | | *https://make.events/public/user/cdj8tr* | |
| Снимок экрана (скриншот), подтверждающий посещение мероприятия | | | |
|  | | | |