Министерство образования и науки Российской Федерации  
Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет  
имени первого Президента России Б.Н. Ельцина»

Институт радиоэлектроники и информационных технологий – РтФ Департамент информационных технологий и автоматики

ОТЧЕТ ПО ПРОЕКТУ

«Маркетинговая аналитика в кибербезопасности»

Тема:

«Сравнительный анализ программных продуктов в области информационной безопасности»

Куратор проекта: Чернышов Юрий Юрьевич \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(подпись)

Студент: РИ-231002 Нижник Евгений Ильич

Студент: РИ-231001 Шадин Роман Викторович\_

Студент: РИ-231002 Бердюгин Кирилл Александрович

Студент: РИ-231001 Задорожный Александр Александрович

Студент: РИ-231001 Жданов Денис Вячеславович

Екатеринбург

2025

# Содержание

[Содержание 2](#_q3g4bciftbi8)

[Введение 3](#_gveh4wmjp811)

[Основная часть 5](#_ug5b6ipp8h6r)

[Итерация 1: 5](#_vxwh8eyam9c9)

[Итерация 2: 6](#_dcu5tvbetwc3)

[Работа над ошибками 6](#_gw3toflrrjb0)

[LLM 7](#_hptc3cv8uof5)

[Киберполигоны 8](#_6b8rzeb5urjk)

[BSS 9](#_oi7gk2e87ga6)

[Итерация 3: 10](#_h09cxk1gwxb)

[Заключение 12](#_g4w13cv03ae6)

[Библиография 13](#_ms24rrax53yr)

[Приложения 14](#_sh0hdxx17yzr)

# 

# 

# Введение

**Цель проекта:**

На основе анализа рынка и решений в области информационной безопасности выделить перспективные направлениях развития для семейства продуктов UDV Group.

**Описание проекта:**

В сфере информационной безопасности постоянно продолжается противостояние между атакующими и защищающейся стороной. Работая в области защиты, необходимо не только реагировать на текущие угрозы, но и предугадывать возможные векторы атак, направляя ресурсы на разработку решений, которые в будущем обеспечат максимальную защиту при минимальных затратах.

Основой этой работы является маркетинговый анализ. В рамках нашего проектного практикума мы проведём исследование текущих решений в области информационной безопасности, сравним их функциональные возможности, проанализируем сильные и слабые стороны, а также выделим перспективные направления развития для продуктов UDV Group.

**Итоги работы:**

В рамках проекта, посвященного маркетинговому анализу решений в области информационной безопасности, была проведена глубокая исследовательская работа, направленная на выявление актуальных функций существующих продуктов и определение перспективных направлений для разработки новых решений в семействе продуктов UDV Group.

Ключевым результатом проекта является отчет, который включает в себя сравнительный анализ существующих решений в области информационной безопасности. Помимо того, можно подчеркнуть некоторые смежные итоги:

1. Повышение квалификации команды проекта: Участники проекта получили возможность углубить свои знания в области информационной безопасности, развить аналитические навыки и научиться работать с разнообразными источниками информации.
2. Развитие навыков исследования и анализа: Команда овладела методами маркетингового анализа, что позволит в дальнейшем более эффективно исследовать рынок и определять тренды в области ИБ.
3. Углубление знаний о текущих трендах и угрозах: Участники проекта ознакомились с современными инструментами атаки и защитной информации, что поможет им быть в курсе последних изменений в области информационной безопасности.
4. Формирование аналитического мышления: Работа над проектом способствовала способности к анализу больших объемов информации, что является важным навыком в сфере ИБ.

Все участники проекта занимают должности аналитиков в рамках выполняемого проекта. Тимлид команды: Нижник Евгений Ильич.

# Основная часть

## Итерация 1:

В первой итерации проекта наша команда сосредоточилась на создании общего аналитического доклада на тему CMDB, который стал бы основой для дальнейшего анализа и консультаций с куратором. Этот подход позволил объединить усилия и знания каждого члена команды, что способствовало более глубокому и всестороннему исследованию темы.

1. Определение целей и задач: На первом собрании команда обсудила основные цели проекта, включая необходимость провести маркетинговый анализ существующих решений в области информационной безопасности и выявить перспективные направления для разработки новых продуктов UDV Group. Члены команды согласовали задачи, которые необходимо решить для достижения этих целей.
2. Сбор информации: Команда начала активный поиск информации, изучая статьи, вебинары и доклады на конференциях. Каждый участник делился найденными материалами в общем чате, что способствовало обмену знаниями и идеями.
3. Написание и редактирование: Члены команды начали совместную работу над текстом доклада, используя облачные инструменты для совместного редактирования. Каждый участник отвечал за написание своих разделов, а затем команда проводила совместные ревизии, внося правки и улучшения.

В ходе консультации были выявлены следующие проблемы:

1. Наличие несостыковок: недостаточно глубокие ревизии привели к расхождениям в некоторых разделах доклада.
2. Недостаточный уклон в маркетинг: Общий доклад больше был похож на образовательный, с общими терминами, производителями и т.д.
3. Недостаточный объем библиографии.

## Итерация 2:

### Работа над ошибками

На данном этапе выполнения проекта команда работала над устранением ошибок предыдущей итерации:

1. Разбиение членов команды на отдельные темы: Данное действие помогло избежать несостыковок в анализе данных, а также расширить круг тем в рамках проекта
2. Консультация с куратором в конце первой итерации помогла выявить недочеты в анализе, и глубже влиться в маркетинговый анализ.
3. Более тщательный поиск информации и выбор более достоверных источников.

Как сказано выше, было принято решение пересмотреть стратегию исследования, а именно, разбиться на различные темы для более широкого охвата анализируемой области кибербезопасности. В конечном итоге всего было рассмотрено несколько лидирующих решений для компании UDV Group:

1. LLM
2. Киберполигоны
3. BSS

Рассмотрим их более подробно:

### LLM

**Большие языковые модели** (Large Language Models, LLM) – это сложные нейронные сети, обученные на больших массивах текстовых данных, способные решать задачи анализа, обработки и генерации текстовой информации. Эти модели, включая архитектуры вроде GPT, BERT и их аналоги, выделяются способностью понимать контекст и семантические связи, что делает их эффективным инструментом для работы с неструктурированными данными.

Решения на основе LLM предполагают использование нейронных сетей с множеством параметров; модели обучаются на больших объемах текстовых данных для понимания и генерации естественного языка и работают, анализируя контекст и паттерны в тексте, что позволяет им предсказывать следующее слово или фразу на основе предыдущих. Продукты на основе LLM используются в различных областях, включая создание чат-ботов, автоматический перевод, генерацию контента, анализ текста и поддержку программирования, что делает их полезными для бизнеса, образования и технологий.

По данным РБК, объем российского рынка LLM-продуктов для бизнеса (Large Language Model, «большая языковая модель») по итогам 2024 года составит 35 млрд руб., подсчитали в Центре искусственного интеллекта МТС (MTS AI). До 2028 года этот показатель будет расти в среднем на 25% в год, прогнозируют аналитики центра. При этом объем рынка LLM-продуктов в мире в 2024 году составит $6,4 млрд (665,5 млрд руб. по текущему курсу), следует из исследований [MarketsandMarkets](https://dzen.ru/away?to=https%3A%2F%2Fwww.marketsandmarkets.com%2FMarket-Reports%2Flarge-language-model-llm-market-102137956.html), [BIS Research](https://dzen.ru/away?to=https%3A%2F%2Fbisresearch.com%2Findustry-report%2Flarge-language-model-market.html) и [Polaris Market Research](https://dzen.ru/away?to=https%3A%2F%2Fwww.polarismarketresearch.com%2Fpress-releases%2Flarge-language-model-llm-market). В ближайшие годы темпы роста мирового рынка будут варьироваться в диапазоне 30–35%.

В данный момент Российский сегмент больших языковых моделей отстает. Аналитики MTS AI среди основных факторов, сдерживающих рост российского рынка LLM-продуктов, называют санкционные ограничения и дефицит квалифицированных специалистов в области искусственного интеллекта и машинного обучения.

Стоит сказать, что данный вектор развития может положительно сказаться на росте компании, а также позволит выйти в лидеры на Российском рынке.

### Киберполигоны

**Киберполигоны** – платформы для проведения тренировок по информационной безопасности разного формата. Он предоставляет эмуляцию бизнес-процессов и информационной инфраструктуры типовых организаций различных отраслей (кредитно-финансового сектора, промышленности, энергетики, транспорта, связи). Участникам киберучений предоставляются технологии и инструменты для получения и отработки практических навыков по защите от кибератак.

Чем крупнее и сложнее виртуальная инфраструктура, тем больше вариантов проведения тренировок (обучений, учений режима «авария», образовательных мероприятий) и тем ближе к реальности и полезнее опыт участия. Стоит отметить, что количество регистрируемых событий безопасности растет. Согласно отчету «Кибератаки на российские компании в 2023 г.», подготовленному компанией «Солар», количество выявленных событий безопасности в четвертом квартале 2023 г. увеличилось на 68% по сравнению с аналогичным периодом предыдущего года.

Объем мирового рынка киберполигонов в 2023 г. оценивался в 2,4 млрд долл. Ожидается, что к 2032 г. он достигнет 9,2 млрд долл., среднегодовой темп роста составит 21%. Такие данные приводит исследовательская компания Dataintelo в своем отчете Cyber Range Market за прошлый год. Эти совокупные цифры включают все сегменты по типу киберполигонов и сферам применения. Точных данных в открытом доступе о российском рынке киберполигонов нет, однако есть основания считать, что он имеет схожие тенденции устойчивого роста.

Стоит также отметить острую нехватку квалифицированных специалистов по информационной безопасности. По данным совместного опроса «СерчИнформ» и hh.ru за 2022 г., 54% российских компаний испытывают нехватку ИБ-кадров, а среди субъектов КИИ таковых 48%. В таких условиях возникает потребность относительно быстро доучить и переучить большое количество людей. Следовательно, развитие тренировочных платформ поможет минимизировать проблему с дефицитом кадров за счет оптимизации процесса обучения.

### BSS

**Breach Simulation Systems** (BSS) — это специальные инструменты и платформы, предназначенные для имитации кибератак на информационные системы организаций. Основная цель BSS — выявление уязвимостей и слабых мест в системах безопасности до того, как злоумышленники смогут их использовать. Это проактивный подход к кибербезопасности, который позволяет организациям принимать меры для защиты своих данных и инфраструктуры. Можно сказать, что различные BSS составляют перечень инструментов Breach and Attack Simulation(BAS). Некоторые сведения, представленные в аналитике, будут касаться именно BAS, в связи с узконаправленностью темы BSS.

Согласно исследованию «Automated Breach and Attack Simulation (BAS) Market Size And Forecast» рынок BAS оценивался в 130,82 млн долларов США в 2019 году и, по прогнозам, достигнет 1572,59 млн долларов США к 2027 году, увеличиваясь в среднем на 36,47 % с 2020 по 2027 год. По данным [прогноза развития рынка кибербезопасности в РФ на 2023-2027 годы](https://www.csr.ru/upload/iblock/0da/cl25xkzy12if5l4xs425yi25ezp1a11z.pdf) от ЦСР, рост объема рынка кибербезопасности за период 2022–2027 года ожидается в районе 24 % CAGR. При этом на основе данных о продажах дистрибьютора «Тайгер Оптикс» можно предполагать, что объем рынка BAS в России составляет порядка 2–2,5 млн долларов США в годовом выражении.

В России сегмент рынка продуктов Breach and Attack Simulation находится на ранней стадии развития. Продукты только появляются на рынке, многие компании только проводят пилотные тесты, однако интерес со стороны заказчиков увеличивается. При этом на российском рынке присутствуют как отечественные вендоры (ООО «Контролхак»), так и зарубежные (Cronus Cyber Technologies, Cymulate, Pcysys, Picus Security). По мнению Романа Богомолова, в России не более 10 заказчиков используют подобные системы на текущий момент.

Учитывая масштаб мировых бюджетов данной отрасли, можно сказать, что эта технология уже успела зарекомендовать себя на рынке, а её начальная стадия развития позволит в короткие сроки догнать конкурентные компании.

## Итерация 3:

В третьей итерации проекта команда работала над итоговым отчетом, который был основан на аналитических данных, собранных во второй итерации. Этот этап сосредоточился на окончательной подготовке и доработке документа, а также на представлении результатов работы, создании защитного слова и презентации.

Работа третьей итерации:

1. Обсуждение результатов второй итерации: На первом собрании третьей итерации команда провела детальный анализ результатов, полученных во второй итерации. Каждый участник предоставил свои выводы и ключевые находки по отдельным темам, над которыми он работал. Это включало в себя анализ существующих продуктов и текущих трендов в области информационной безопасности.
2. Интеграция аналитических данных: Команда объединила все собранные данные и выводы в единый документ. Участники совместно работали над тем, чтобы структурировать отчет, выделив основные разделы, такие как:
   * Введение и цели работы.
   * Сравнительный анализ существующих решений.
   * Обзор текущих трендов.
   * Рекомендации по разработке или приобретении новых продуктов для UDV Group.
3. Редактирование текста: Члены команды провели совместное редактирование итогового отчета, уделяя внимание как содержательной части, так и стилю изложения. Используя облачный инструмент Google Диск, участники могли равноправно вносить правки и комментарии, что способствовало более эффективному взаимодействию.
4. Подготовка к презентации: В заключение, команда подготовила презентацию, которая обобщала основные выводы и рекомендации из итогового отчета.
5. Презентация итогового отчета: Команда провела встречу с куратором, на которой представила итоговый отчет и результаты проведенного анализа. Участники ответили на вопросы и обсудили возможные дальнейшие шаги, основанные на полученных рекомендациях.

Таким образом, третья итерация работы команды была сосредоточена на окончательной подготовке и представлении итогового отчета, что позволило команде продемонстрировать результаты своего труда и заложить основу для дальнейших действий в области разработки новых продуктов UDV Group.

# 

# Заключение

В заключение, результаты нашего анализа представляют собой рекомендации для дальнейшего развития продуктов и услуг UDV Group. Мы уверены, что реализация предложенных инициатив позволит значительно повысить конкурентоспособность компании и улучшить качество предоставляемых решений в области информационной безопасности. Команда готова продолжать работу над этими направлениями и обеспечивать поддержку в их реализации.

Кроме того, стоит отметить, что в процессе работы над проектом участники команды продемонстрировали значительный личностный рост и профессиональное развитие. Каждый член команды приобрел новые знания и навыки, улучшил свои аналитические способности и научился работать в условиях динамичной и многозадачной среды.

# 

# 

# Библиография

Яндекс Дзен: официальный сайт. - Москва. - Обновляется в течение суток. - URL: [https://dzen.ru](https://dzen.ru/a/Z0VcFOh0TidNfkp9) (дата обращения: 18.01.2025). - Текст: электронный.

Перспективный мониторинг: официальный сайт. - Москва. -

Обновляется в течение суток. - URL: [https://amonitoring.ru](https://amonitoring.ru/article/kiberpoligony-v-stadii-rosta-connect/?ysclid=m45klsvr1i986378919) (дата обращения: 18.01.2025). - Текст: электронный.

TAdvister: новостной сайт. - Обновляется в течение суток. - URL: [https://www.tadviser.ru](https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A7%D0%B8%D1%81%D0%BB%D0%BE_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8_%D0%B8_%D0%B2_%D0%BC%D0%B8%D1%80%D0%B5?ysclid=m45mtrvawl563743242) (дата обращения: 18.01.2025). - Текст: электронный.

Anti-Malware: новостной сайт. - Обновляется в течение суток. - URL: <https://www.anti-malware.ru/analytics/Market_Analysis/Breach-and-Attack-Simulation-Market-Overview#part4> (дата обращения:18.01.2025). - Текст: электронный.

Anti-Malware: новостной сайт. - Обновляется в течение суток.URL: <https://www.anti-malware.ru/analytics/Technology_Analysis/Breach-and-Attack-Simulation> (дата обращения: 18.01.2025). - Текст: электронный.

Фонд «Сколково»: официальный сайт. - Обновляется в течение суток. - URL: <https://navigator.sk.ru/orn/1123572> (дата обращения: 18.01.2025). - Текст: электронный.

# 

# 

# Приложения

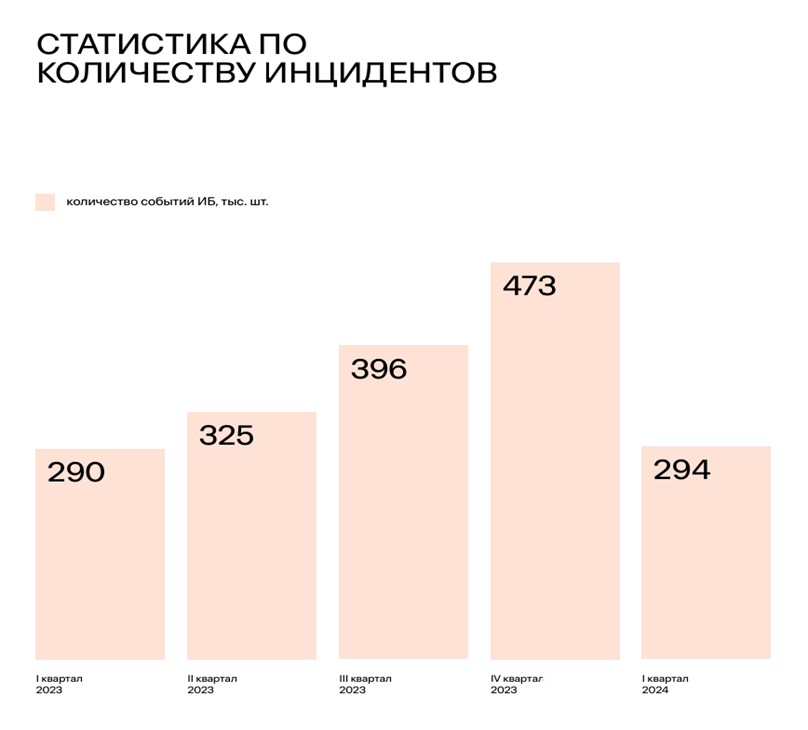


рис. 1 - Количество инцидентов ИБ за 2023г.



рис. 2 - Мировой показатель использования BSS

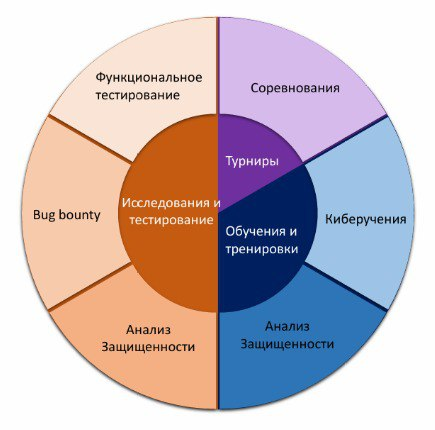


рис. 3 - Возможности киберполигонов

[Прогноз развития рынка кибербезопасности в Российской Федерации на 2023–2027 годы](https://www.csr.ru/upload/iblock/0da/cl25xkzy12if5l4xs425yi25ezp1a11z.pdf) – ссылка на отчет.