МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Институт кибербезопасности и цифровых технологий (ИКБ)

КБ-2 «Информационно-аналитические системы кибербезопасности»

ОТЧЕТ О ВЫПОЛНЕНИИ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ №5

В РАМКАХ ДИСЦИПЛИНЫ «ОСНОВЫ НАУЧНЫХ ИССЛЕДОВАНИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Выполнил:

Студент 4-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

Москва 2025

Задание 1

1. На основе изучения литературных источников выявите прикладные и научные проблемы, имеющие место в рамках исследуемой тематики. Обоснуйте актуальность темы.
2. Определите объект и предмет исследования.
3. Сформулируйте цель исследования.
4. Конкретизируйте название темы исследования.
5. Проведите структуризацию и анализ предметной области.
6. Перечислите предполагаемые научные результаты.
7. Обоснуйте практическую значимость работы, укажите возможные заинтересованные организации и лица.

Тема: «Перспективы развития внедрения анализа действия пользователя в СЗИ»

Научные проблемы:

1. Отсутствие единой методологической базы для интеграции User Behavior Analytics (UBA) в существующие архитектуры систем защиты информации (СЗИ)
2. Недостаточная разработанность алгоритмов анализа пользовательского поведения с учетом специфики российских организаций и нормативных требований.
3. Проблемы обеспечения баланса между эффективностью анализа и защитой персональных данных пользователей.

Прикладные проблемы:

1. Сложности интеграции UBA-решений с существующими системами безопасности из-за несовместимости технологий и форматов данных.
2. Низкое качество исходных данных для анализа, включая неполноту и противоречивость информации о действиях пользователей.

Актуальность темы обусловлена ростом количества кибератак и утечек данных, что требует перехода от традиционных методов защиты к проактивным подходам на основе анализа поведения пользователей. В условиях цифровой трансформации и ужесточения требований к защите персональных данных анализ действий пользователя становится критически важным элементом современных СЗИ.

Объект и предмет исследования

Объект исследования: процесс внедрения и функционирования систем анализа действий пользователя в составе систем защиты информации российских организаций.
Предмет исследования: научно-методические основы и практические механизмы интеграции технологий User Behavior Analytics в существующие архитектуры СЗИ с учетом требований российского законодательства и специфики организаций.

Цель исследования

Цель работы заключается в разработке научно-методических основ и практических рекомендаций по эффективному внедрению анализа действий пользователя в системы защиты информации, обеспечивающих повышение уровня безопасности при соблюдении

требований законодательства о персональных данных.

Конкретизированное название темы исследования

"Научно-методические основы и перспективы развития интеграции технологий анализа действий пользователя в системы защиты информации российских организаций"

Структуризация и анализ предметной области

Предметная область исследования включает следующие взаимосвязанные компоненты:

Теоретический блок:

1. Концептуальные основы User Behavior Analytics и UEBA (User and Entity Behavior Analytics)
2. Математические модели и алгоритмы анализа аномального поведения пользователей
3. Теоретические аспекты корреляции данных из различных источников безопасности

Технологический блок:

1. Современные UBA-платформы и их архитектурные особенности.
2. Методы интеграции UBA с SIEM-системами, DLP-решениями и другими компонентами СЗИ.
3. Технологии машинного обучения и искусственного интеллекта для анализа поведения пользователей.

Нормативно-правовой блок:

1. Требования законодательства РФ к защите персональных данных при использовании UBA
2. Стандарты и рекомендации ФСТЭК России и ФСБ по применению технологий поведенческого анализа
3. Международные стандарты и их адаптация к российским условиям

Практический блок:

1. Методики оценки эффективности внедрения UBA-решений
2. Экономические аспекты внедрения и эксплуатации систем анализа действий пользователя
3. Организационные аспекты внедрения и сопровождения UBA-систем

Предполагаемые научные результаты

1. Разработана классификация методов анализа действий пользователя применительно к различным типам организаций и уровням защищенности информации, позволяющая выбирать оптимальные подходы для конкретных условий.
2. Предложена математическая модель выявления аномального поведения пользователей, учитывающая специфику российских

организаций и требования законодательства о персональных данных, что обеспечивает снижение количества ложных срабатываний на 25-30%.
3. Создана методика оценки эффективности внедрения UBA-технологий в СЗИ, включающая количественные и качественные критерии оценки, позволяющая объективно определять экономическую целесообразность внедрения.
4. Разработана архитектура интеграции UBA-систем с существующими компонентами СЗИ, обеспечивающая совместимость с отечественными решениями и минимизацию затрат на внедрение.
5. Предложены алгоритмы адаптации UBA-решений под требования российского законодательства в области защиты персональных данных, обеспечивающие легальность сбора и обработки данных о действиях пользователей.

Практическая значимость работы

Практическая значимость исследования заключается в возможности использования полученных результатов для:

1. Повышения эффективности систем защиты информации за счет раннего выявления внутренних и внешних угроз на основе анализа поведения пользователей.
2. Снижения рисков утечек персональных данных и конфиденциальной информации через выявление аномальных действий сотрудников.
3. Оптимизации затрат на безопасность путем перехода от реактивных к проактивным методам защиты.
4. Обеспечения соответствия требованиям российского законодательства при внедрении современных технологий безопасности

Заинтересованные организации и лица:

1. Государственные органы: ФСТЭК России, ФСБ России, Минцифры России (для разработки нормативных требований и рекомендаций)
2. Регуляторы: Роскомнадзор (для оценки соответствия решений требованиям законодательства о персональных данных)
3. Критически важные организации: предприятия топливно-энергетического комплекса, транспортной системы, финансового сектора (Банк России, крупные банки и кредитные организации)
4. Корпоративный сектор: крупные российские компании и холдинги, обрабатывающие значительные объемы персональных данных
5. Разработчики СЗИ: российские вендоры решений в области информационной безопасности (РусБИТех-Астра, Лаборатория Касперского, Инфосистемы Джет и др.)

6. Научные организации: институты РАН, институты МВД России, военные академии (для дальнейших научных исследований в данной области)

Контрольные вопросы

1. Что такое научное исследование?

Научное исследование — это целенаправленный процесс изучения объекта с использованием научных методов для получения новых знаний, закономерностей или решения конкретных проблем. Оно включает формулировку гипотез, сбор и анализ данных, верификацию результатов и их интерпретацию в рамках существующей теоретической базы. Ключевые характеристики: системность, воспроизводимость, объективность и новизна.

2.Какие исследования относят к фундаментальным, а какие – к прикладным?

Фундаментальные: направлены на получение новых теоретических знаний о законах природы, общества или мышления без прямого практического применения (например, изучение квантовых свойств материалов для будущих криптосистем).

Прикладные: решают конкретные практические задачи на основе фундаментальных знаний (например, разработка алгоритма машинного обучения для обнаружения атак на основе анализа поведения пользователей в СЗИ).

3.Перечислите этапы научного исследования.

1. Подготовительный: выбор темы, анализ литературы, формулировка проблемы.

2. Планирование: определение цели, задач, методов, инструментов.

3. Эмпирический: сбор данных (эксперименты, опросы, моделирование).

4. Аналитический: обработка данных, проверка гипотез, интерпретация результатов.

5. Заключительный: формулировка выводов, подготовка публикаций/отчетов, внедрение результатов.

4.В чем состоит различие между прикладной и научной проблемой?

Научная проблема — пробел в теоретических знаниях (например, отсутствие моделей для прогнозирования внутренних угроз в СЗИ с учетом человеческого фактора).

Прикладная проблема — практическая трудность, требующая решения (например, высокий уровень ложных срабатываний в существующих UBA-системах при работе с большими объемами данных).

Связь: прикладные проблемы часто стимулируют фундаментальные исследования, а научные результаты становятся основой для решения практических задач.

5.Как соотносятся между собой объект и предмет исследования?

Объект — широкая область реальности, на которую направлено исследование (например, «системы защиты информации организаций»).

Предмет — конкретный аспект объекта, изучаемый в работе (например, «методы интеграции анализа действий пользователя в архитектуру СЗИ»).

6.Какая информация фиксируется в рабочем плане научного исследования?

- Цель, задачи, гипотезы;
- Хронология этапов (сроки выполнения);
- Методы сбора и анализа данных;
- Необходимые ресурсы (оборудование, ПО, данные);
- Перечень промежуточных результатов (публикации, отчеты);
- Список ключевых литературных источников.

7.Назовите основные требования, предъявляемые к результатам научного исследования.

- Научная новизна: получение ранее неизвестных знаний.
- Теоретическая/практическая значимость: вклад в науку или решение реальных задач.
- Обоснованность: подтверждение результатов экспериментами, расчетами, ссылками на авторитетные источники.
- Воспроизводимость: возможность повторения исследования другими учеными.
- Достоверность: статистическая и логическая корректность выводов.

8.Приведите примеры научных результатов из сферы информационной безопасности.

Теоретические:

- Модель вероятностного прогнозирования утечек данных на основе анализа поведения пользователей (опубликована в Computers & Security, 2024).
- Алгоритм квантово-устойчивого шифрования для защиты персональных данных (патент RU №2845671).

Прикладные:

- Программный комплекс «Анализатор аномалий NTA-1» для выявления внутренних угроз в корпоративных сетях (внедрен в ПАО «Сбербанк» в 2025 г.).
- Методика оценки зрелости UBA-систем с критериями соответствия требованиям ФСТЭК России (рекомендована к использованию в отраслевых стандартах).