ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПРИНЯТИЕ РЕШЕНИЙ
ARTIFICIAL INTELLIGENCE AND DECISION MAKING

УДК 004.85 **DOI: 10.18413/2518-1092-2026-11-2-0-6**

Чмыхало Д.С.
Газизов А.Р.
Легонько О.Л.

СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ РЕАГИРОВАНИИ НА УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФГБОУ ВО «Донской государственный технический университет» (ДГТУ)
пл. Гагарина, 1, г. Ростов-на-Дону, 344002, Россия

e-mail: chmykhalo3009@gmail.com, agazizov@donstu.ru, olga_cvetkova@mail.ru

Аннотация
В современных условиях практически всеобъемлющей цифровизации обеспечение информационной безопасности предприятий и организаций различных форм собственности и областей деятельности становится все более актуальной задачей, требующей использования передовых методов обнаружения и реагирования на угрозы. В данной статье представлена разработанная авторами система поддержки принятия решений, предназначенная для выявления и классификации угроз информационной безопасности, а также автоматизации формирования сценариев реагирования. Предложенная архитектура представляет сбой модульную структуру, сочетающую методы машинного обучения, экспертные системы и инструменты объясняющего искусственного интеллекта, что повышает точность идентификации угроз, оценки рисков и усиливает степень доверия специалистов к автоматическим решениям, сформированным интеллектуальной частью системы. В рамках исследования выполнена разработка и тестирование системы с использованием набора данных UNSW-NB15, который содержит информацию о сетевом трафике, сгенерированную в лабораторных условиях. Представленные результаты демонстрируют перспективы внедрения разработанной системы в службы безопасности предприятий, способствуя минимизации ущерба от реализации атак на информационную инфраструктуру в корпоративных и государственных информационных системах. Предложена идея дальнейшего развития системы с учетом расширения датасетов, включающее новые типы угроз и сценариев реагирования, и внедрение онлайн-обучения для адаптации моделей к динамично меняющейся ситуации безопасности.

Ключевые слова: система поддержки принятия решений; технологии искусственного интеллекта; информационная безопасность; защита информации; угроза информационной безопасности

Для цитирования: Чмыхало Д.С., Газизов А.Р., Легонько О.Л. Система поддержки принятия решений при реагировании на угрозы информационной безопасности // Научный результат. Информационные технологии. – Т.11, №2, 2026. – С. 62-76. DOI: 10.18413/2518-1092-2026-11-2-0-6

Chmykhalo D.S.
Gazizov A.R.
Legonko O.L.

DECISION SUPPORT SYSTEM FOR RESPONDING TO INFORMATION SECURITY THREATS

Don State Technical University
1 Gagarin square, Rostov-on-Don, 344003, Russia

e-mail: chmykhalo3009@gmail.com, agazizov@donstu.ru, olga_cvetkova@mail.ru

Abstract
In today's increasingly digitalized world, ensuring information security for enterprises and organizations across various business types and industries is becoming an increasingly pressing issue, requiring advanced threat detection and response methods. This article presents a decision support system developed by the authors for identifying and classifying information security threats and automating the generation of response scenarios. The proposed architecture is a modular structure combining machine learning methods, expert systems, and explanatory artificial intelligence tools, which improves the accuracy of threat identification and risk assessment and enhances the confidence of specialists in the automated decisions generated by the system's intelligent component. The study included developing and testing the system using the UNSW-NB15 dataset, which contains network traffic information generated under laboratory conditions. The presented results demonstrate the potential for implementing the developed system in enterprise security services, helping to minimize damage from attacks on the information infrastructure of corporate and government information systems. An idea is proposed for further development of the system, taking into account the expansion of datasets, including new types of threats and response scenarios, and the introduction of online learning to adapt models to the dynamically changing security situation.
Keywords: expert system; artificial intelligence technologies; information security; information protection; information security threat
For citation: Chmykhalo D.S., Gazizov A.R., Legonko O.L. Decision Support System for Responding to Information Security Threats // Research result. Information technologies. – T.11, №2, 2026. – P. 62-76. DOI: 10.18413/2518-1092-2026-11-2-0-6

ВВЕДЕНИЕ

В настоящее время в условиях масштабного использования электронного документооборота во всех подразделениях и бизнес-процессах предприятия, постоянного совершенствования угроз и расширения видов атак на информационную инфраструктуру, появляется необходимость решения актуальной задачи разработки новых эффективных средств защиты информационной инфраструктуры [1]. Решению этой задач посвящено множество научных работ, в которых авторы рассматривают одно из самых перспективных направлений в этой отрасли – это внедрение технологий искусственного интеллекта.

Одной из заслуживающих научных работ в этой области является статья [2], в которой авторы проанализировали множество научных публикаций за 2018-2023 годы. Они отмечают, что при построении систем защиты с использованием искусственного интеллекта в целом наблюдается повышение их эффективности. Это происходит за счет того, что ряд операций анализа угроз выполняется системой, а не человеком. Однако, вместе с тем, исследователи говорят и о возможных рисках: для успешной работы таких систем нужны качественные обучающие данные, что является основой для проведения дальнейших исследований в этом направлении.

В научных исследованиях [3-6] авторы анализируют возможности применения искусственного интеллекта в сфере защиты конфиденциальной информации, для выявления аномалий в информационных системах, и поднимают очень важный вопрос, который, по сути, должен вставать во всех областях при использовании искусственного интеллекта – необходимость анализа и контроля решений, принимаемых системой, и акцентируют внимание на проблеме обеспечения прозрачности процессов принятия этих решений. Эти исследования демонстрируют,

что технологии искусственного интеллекта обладают потенциалом, позволяющем значительно повысить эффективность автоматизированных систем защиты, обеспечить работу в режиме реального времени и снизить влияние человеческой ошибки.

Далее стоит упомянуть исследования, представленные в работах [7, 8], в которых помимо обсуждения преимуществ, рассматриваются также проблемы и ограничения, связанные с внедрением методов машинного обучения, глубокого обучения и обучения с подкреплением в информационную безопасность. Авторы указывают, что, хотя эти технологии улучшают обнаружение угроз, их внедрение требует выявления возникающих уязвимостей и потенциального неправомерного использования, чтобы системы можно было защищать более прозрачно и эффективно.

Другим примером, подтверждающем актуальность данной темы является работа [9], в которой авторы провели обзор литературы с использованием данных из таких поисковых систем, как Google Scholar, ResearchGate, ScienceDirect, IEEE Xplore, Digital Library и Microsoft Academic, для оценки возможностей искусственного интеллекта в информационной безопасности. И в итоге, авторы сделали основной вывод, заключающийся в том, что использование искусственного интеллекта имеет значительные преимущества по сравнению с традиционными подходами при защите информации.

Наконец, еще одним уместным примером, который стоит упомянуть в контексте рассматриваемой задачи, является научная работа [10], в котором представлен систематический обзор текущего состояния объяснимого искусственного интеллекта (Explainable Artificial Intelligence, XAI) и его актуальности для информационной безопасности. На основе проводимых исследований авторы приходят к выводу, что разработка и применение объяснимого искусственного интеллекта могут значительно улучшить как понимание, так и эффективность защитных мер.

Множество современных предприятий из различных отраслей деятельности используют системы управления информацией о безопасности (Security Information and Event Management, SIEM), которые помогают отслеживать и защищать их информационную инфраструктуру. Однако у этих систем есть свои ограничения: они часто бывают дорогими и требуют значительных усилий для адаптации под особенности конкретного предприятия. Кроме того, в некоторых случаях возникает зависимость от определенных торговых марок, что создает дополнительные сложности. Таким образом, перспективным решением становится создание собственной, индивидуально разработанной системы поддержки принятия решений (СППР).

Изучению вопросов применения систем поддержки принятия решений в различных областях посвящено множество научных работ авторов. Одной из популярных областей деятельности, в которую активно внедряются технологии искусственного интеллекта является сфера информационной безопасности.

Научная статья [11] посвящена вопросу использования систем поддержки принятия решений в различных отраслях экономики. Автор выполнил анализ некоторых реализованных проектов развития систем поддержки принятия решений на российских предприятиях.

В статье [12] поднимается вопрос синтеза технологий искусственного интеллекта и СППР, который позволит оптимизировать процесс принятия решений на основе взаимодействия нейронных сетей с нечеткими (размытыми) системами и элементами управления. Автор на примере задачи управления проектами показывает основные роли, которые может исполнять искусственный интеллект (ассистент руководителя, советник, методолог). Предлагаются варианты использования интеллектуальных систем и типов решений в проектной деятельности.

В статье [13] рассматриваются подсистема принятия решений и использование методов искусственного интеллекта для реализации этапов принятия решений в ситуационном центре.

В работе [14] приводится описание системы поддержки принятия решений при обеспечении информационной безопасности системы верхнего уровня автоматизированной системы

управления технологическими процессами атомной электростанции. Задача системы заключается в поиске и ранжировании конфигураций средств защиты информации.

Работа [15] посвящена исследованию вопроса актуальности внедрения систем поддержки принятия решений в процессы управления современными предприятиями. Рассмотрена классификация видов современных систем поддержки принятия решений, а также сформулированы особенности и проблемы применения искусственных нейронных сетей в системах поддержки принятия решений.

В статье [16] рассматривается задача обеспечения информационной безопасности автоматизированных систем управления технологическими процессами промышленных объектов. Исследования в статье направлены на совершенствование процедуры количественной оценки рисков информационной безопасности. Представлены архитектура интеллектуальной системы поддержки принятия решений и программная реализация инструментальных средств автоматизации моделирования сценариев атак и оценки рисков.

В научной работе [17] выполнен обзор публикаций, посвященных проблеме эффективного применения обученных искусственных нейронных сетей в решении задач классификации, прогнозирования и управления. Рассмотрены особенности и выполнен сравнительный анализ популярных структур нейронных сетей и методик формирования обучающих выборок.

В работе [18] рассматривается задача проектирования информационной системы поддержки принятия решений при разработке систем защиты объектов информатизации. Предлагается использование методов разработки моделей функционирования защищенных информационных систем в условиях деструктивного воздействия на основе байесовских сетей.

В работе [19] предложена архитектура прототипа интеллектуальной системы для автоматизированной поддержки принятия решений, моделирования сценариев атак и оценки рисков информационной безопасности промышленной системы управления, что повышает точность и скорость оценки рисков и помогает выбрать эффективные меры защиты на всех этапах жизненного цикла объекта и систем его защиты.

В статье [20] предложена методика оценки защищенности сложных систем с системой поддержки принятия решений, основанная на SWOT-анализе и логико-вероятностном методе, для выявления угроз нарушения критических свойств средств криптографической защиты. Эта модель позволяет оперативно обнаруживать объекты в опасном состоянии и информировать о необходимости мер безопасности.

Целью исследования, проводимого в настоящей статье, является разработка концептуального проекта системы поддержки принятия решений, предназначенной для автоматизации процесса принятия решений в условиях воздействия угроз информационной безопасности на инфраструктуру предприятия. При этом объектом исследования будут выступать процессы реагирования на угрозы информационной безопасности, а предметом исследования – проект системы поддержки принятия решений при реагировании на угрозы информационной безопасности.

АРХИТЕКТУРА ПРОЕКТИРУЕМОЙ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

Архитектура проектируемой системы поддержки принятия решений построена из следующих основных модулей (рисунок 1):

1. Модуль сбора данных выполняет автоматический сбор конфигурационных параметров источников данных (журналы событий, данные о сетевом трафике, данные о конфигурации и пользователях).

Модуль использует протоколы и программный интерфейс (Application Programming Interface, API) для интеграции с системами мониторинга и управления событиями, системами обнаружения

и предотвращения вторжений, антивирусным программным обеспечением, системами управления доступом.

Передает информацию о событиях и инцидентах в Модуль обнаружения угроз.

2. Модуль обнаружения угроз выполняет идентификацию и классификацию угроз на основе информации о событиях и инцидентах (от Модуля сбора данных), информации о типах угроз и сигнатурах атак (из Базы данных).

Передает перечень обнаруженных угроз с их классификацией в Модуль оценки рисков.

3. Модуль оценки рисков выполняет оценку уровня риска для каждой угрозы (высокий, средний, низкий) на основе перечня обнаруженных угроз (от Модуля обнаружения угроз), информации о ценности активов предприятия (из Базы данных) и информация о вероятностях реализации угроз (из Базы данных).

Передает результаты оценок уровней риска для обнаруженных угроз в Модуль поддержки принятия решений.

Возвращает оператору системы (сотруднику службы безопасности предприятия) результаты оценки.

4. Модуль поддержки принятия решений на основе оценок рисков (от Модуля оценки рисков), сценариев реагирования на угрозы и их эффективности (из Базы знаний) и исторических данных о последствиях прошлых инцидентов (из Базы данных), вырабатывает рекомендуемые сценарии реагирования на угрозы.

Возвращает оператору системы (сотруднику службы безопасности предприятия) рекомендуемые сценарии реагирования на угрозы.

При необходимости оператор системы может выполнить уточнение рекомендуемых сценариев путем взаимодействия с Модулем поддержки принятия решений.

Также Модуль поддержки принятия решений передает информацию о необходимых автоматических действиях в системы управления и безопасности для немедленного выполнения. Эти действия могут включать блокировку подозрительных IP-адресов, отключение уязвимых сервисов и другие меры, направленные на быстрое устранение угроз. Передача этой информации обеспечивает оперативное реагирование на инциденты, минимизируя потенциальные убытки и риски для предприятия.

5. Модуль управления знаниями включает в себя Базу данных и Базу знаний, которые используются Модулем обнаружения угроз, Модулем оценки рисков и Модулем поддержки принятия решений.

Предлагаемая архитектура обеспечивает системный подход к автоматизации процессов выявления и реагирования на угрозы информационной безопасности с использованием современных методов анализа данных, моделирования и оптимизации.

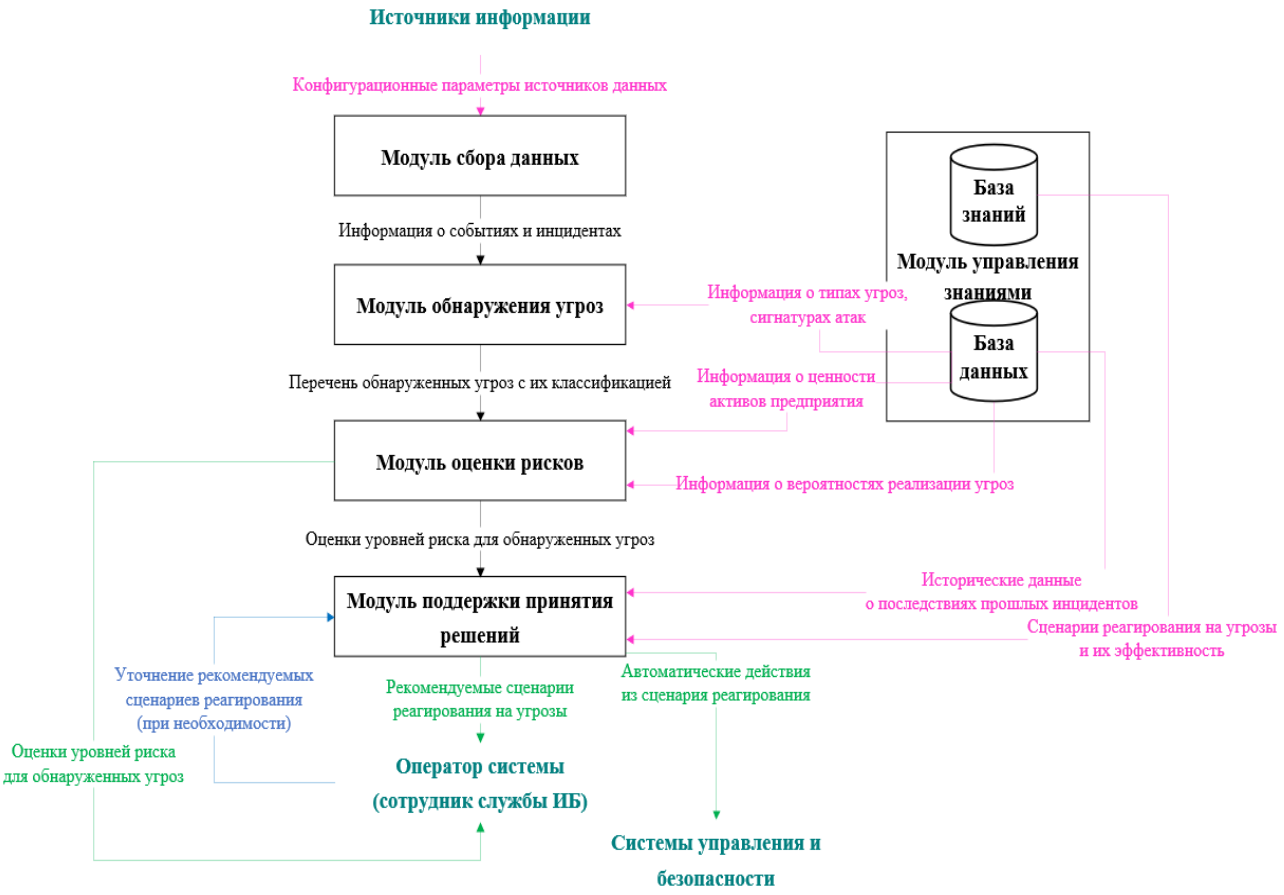

Рис. 1. Архитектура системы поддержки принятия решений при реагировании на угрозы информационной безопасности

Fig. 1. Architecture of the decision support system for responding to information security threats

МЕТОДЫ РЕАЛИЗАЦИИ МОДУЛЕЙ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ПРИ РЕАГИРОВАНИИ НА УГРОЗЫ

1. Модуль сбора данных.

Модуль сбора данных отслеживает сетевой трафик, действия пользователей, системные логи и другие источники информации, выполнят сбор данных из сетевых устройств, серверов, приложений и устройств конечных пользователей. Затем собранные данные проходят первичную фильтрацию для удаления шумов и нерелевантной информации. Например, исключаются незначительные события.

Далее из каждого события определяются ключевые признаки, которые характеризуют его с точки зрения безопасности информации.

После обработки каждое событие представляется в виде набора (вектора) числовых значений признаков.

2. Модуль обнаружения угроз.

Модуль обнаружения угроз предлагается построить на основе использования модели градиентного бустинга XGBoost (eXtreme Gradient Boosting), которая позволяет получить предсказания типов угроз (классов атак) для каждого сетевого события на основе обучения системы по признакам атак, включая вероятности принадлежности к каждому из классов угроз, что обеспечивает интерпретируемость результатов через такие метрики точности, как accuracy, precision, recall и confusion matrix. Эти предсказания затем передаются в Модуль оценки рисков для расчета уровня угрозы.

3. Модуль оценки рисков.

В Модуле оценки рисков выполняется аналитический расчет уровня риска по следующей формуле:

уровень риска = вероятность угрозы × потенциальный ущерб,

где вероятность угрозы – значения в диапазоне от 0 до 1;

потенциальный ущерб – значения в условных единицах.

При этом исходными данными являются значения вероятностей реализации угроз и соответствующий им потенциальный ущерб. Эти данные могут быть получены путем проведения экспертной оценки действующей на предприятии системы защиты и взаимодействия с финансово-экономическими подразделениями.

Также, предварительно, специалисты службы защиты информации предприятия должны определить пороговые значения уровня риска, таким образом, чтобы получить результаты оценки риска в качественном виде – в виде категорий риска. Наиболее популярный вариант решения подобной задачи заключается в задании трех категорий: высокий, средний и низкий риск.

4. Модуль поддержки принятия решений.

Модуль поддержки принятия решений предлагается реализовать с помощью машинного обучения на основе модели градиентного бустинга, обученной на исторических данных инцидентов, которая позволит автоматически выявлять закономерности и рекомендовать наиболее подходящие сценарии реагирования. Модель анализирует признаки: класс угрозы, категорию риска, и на выходе формируются рекомендации по сценариям реагирования.

Таким образом, исходя из приведенного описания методов реализации модулей системы поддержки принятия решений, следует, что в проектируемой системе интеллектуальными являются Модуль обнаружения угроз и Модуль поддержки принятия решений (таблица 1).

Таблица 1

Методы реализации модулей системы поддержки принятия решений

Table 1

Methods for implementing modules of the decision support system

Модуль	Входные данные	Выходные данные	Методы
Модуль сбора данных	Данные из источников (логи SIEM, сетевой трафик, действия пользователей, системные логи, конфигурации устройств, серверов и приложений, Threat Intelligence, исторические инциденты)	Нормализованные числовые векторы признаков и текстовые описания событий (логи)	ETL-процессы с использованием библиотек Pandas и NumPy (без применения искусственного интеллекта)
Модуль обнаружения угроз (интеллектуальный)	Структурированные векторы от Модуля сбора данных Информация о типах угроз и сигнатурах атак (для демонстрации используется набор данных UNSW-NB15)	Перечень обнаруженных угроз с их классификацией	Машинное обучение на основе модели градиентного бустинга XGBoost (eXtreme Gradient Boosting)

Модуль	Входные данные	Выходные данные	Методы
Модуль оценки рисков	Перечень обнаруженных угроз с их классификацией Информация о ценности активов предприятия Информация о вероятностях реализации угроз	Оценки уровней риска для обнаруженных угроз	Аналитический расчет уровня риска: уровень риска = вероятность угрозы × потенциальный ущерб
Модуль поддержки принятия решений (интеллектуальный)	Перечень обнаруженных угроз с их классификацией Оценки уровней риска для обнаруженных угроз Реализованные в прошлом сценарии реагирования на угрозы и их эффективность Исторические данных о последствиях прошлых инцидентов	Рекомендуемые сценарии реагирования на угрозы	Машинное обучение на основе модели градиентного бустинга XGBoost (eXtreme Gradient Boosting)

РЕАЛИЗАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

В качестве программного средства реализации проектируемой системы поддержки принятия решений был выбран язык программирования Python – одно из самых популярных и универсальных средств для разработки интеллектуальных систем и анализа данных. Python широко используется в области машинного обучения, обработки данных и искусственного интеллекта благодаря обширной системе библиотек и активному сообществу разработчиков. Для реализации системы используются библиотеки: XGBoost (для модели решений), Pandas и NumPy (для обработки данных), Matplotlib (для визуализации матрицы ошибок), Scikit-learn (для метрик и нормализации).

На начальном этапе необходимо получить данные для обучения интеллектуальных модулей системы. На практике данные для обучения Модуля обнаружения угроз извлекаются из систем мониторинга, SIEM-систем, базы Threat Intelligence, внутренней документации и аналитики безопасности, для обучения Модуля поддержки принятия решений – из логов SIEM-систем, базы данных инцидентов, исторических отчетов внутренних систем, открытых датасетов (таблица 2).

Таблица 2

Данные для обучения интеллектуальных модулей системы поддержки принятия решений (при практической реализации и внедрении системы)

Table 2

Data for intelligent training modules of the decision support system (during practical implementation and introduction of the system)

№	Источник данных	Данные, которые собираются	Цель использования
Модуль обнаружения угроз			
1	Журналы событий системы (лог-файлы)	Временные метки, типы событий, уровни тревоги, детали событий	Обнаружение аномалий и классификация угроз
2	Сетевой трафик	Пакеты данных, источники и назначения, протоколы, объемы	Анализ активности сети, выявление подозрительных соединений
3	Данные о конфигурациях устройств и систем	Настройки, версии, активированные модули, патчи	Идентификация уязвимостей и известных атак
4	Данные о пользователях и их действиях	Время входа/выхода, права доступа, действия пользователя	Детектор подозрительных активностей и инсайдерских угроз
5	Прошлые инциденты, известные угрозы, сигнатуры	Метки угроз, сигнатуры атак, описания, идентификаторы	Обучение модели на известных атаках
6	Информация о текущих сессиях, соединениях	Активные соединения, длительность, попытки входа	Обнаружение аномальной активности, связанной с атакой
Модуль поддержки принятия решений			
7	Логи SIEM-систем	Исторические записи инцидентов, уровни рисков, принятые решения, временные метки, типы угроз	Обучение модели формировать сценарии реагирования на основе комбинации угроз и рисков
8	Базы данных инцидентов (например, NIST, MITRE ATT&CK)	Анонимизированные кейсы инцидентов, метки решений, уровни серьезности, исходы реагирования	Составление обучающего датасета для классификации решений и оценки рисков
9	Исторические отчеты внутренних систем (SOC, firewall)	Отчеты о прошлых инцидентах, экспертные аннотации решений, метрики эффективности реагирования	Анализ паттернов для обучения модели формированию последовательности оптимальных действий
10	Открытые датасеты для машинного обучения	Адаптированные данные о трафике, угрозах и решениях, с балансировкой классов	Начальное обучение и тестирование модели на синтетических/реальных данных

Для демонстрации процессов обучения и тестирования проектируемой системы поддержки принятия решений используется набор данных UNSW-NB15, содержащий информацию о сетевом трафике, сгенерированную в лабораторных условиях Австралийского университета Нового Южного Уэльса (UNSW) с использованием инструмента IXIA PerfectStorm [21]. Набор включает обычный сетевой трафик (нормальные события), и данные девяти атак (Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode and Worms), что делает его полезным для обучения и тестирования систем обнаружения вторжений. В наборе подготовлены обучающий (тренировочный) и тестовый массивы, хранящиеся в двух файлах. Каждое событие описывается 49 признаками, которые включают в себя обычные, потоковые, временные, контентные и другие характеристики трафика.

Для обучения модуля поддержки принятия решений генерируются синтетические исходные данные для моделирования реальных сценариев, где типы угроз и категории риска влияют на рекомендации для специалистов службы безопасности. Было сгенерировано 3000 событий – по 100 событий для каждой из 30 комбинаций (10 типов угроз × 3 категории риска).

В итоге получается, что исходные данные состоят из следующих признаков:

– threat_type – классы событий, которые были предсказаны в результате запуска Модуля обнаружения угроз;

– risk_category – категории рисков ('низкий', 'средний' и 'высокий'), которые были рассчитаны в результате запуска Модуля оценки рисков. При этом учитывались заданные пороги риска (менее 30%, 30-70% и более 70% от стоимости активов соответственно);

– decision – массив заданных рекомендаций по действиям, поставленных в соответствие с комбинациями угроза + риск. Массив формируется на основе анализа экспертных знаний.

В сформированные таким образом синтетические данные необходимо добавить шум для того, чтобы имитировать реальные условия принятия решений в системах обнаружения вторжений. Это позволит учесть не идеальность рекомендаций, которая возможна из-за человеческого фактора или неполной информации, а также снизит вероятность переобучения система, заставляя модель учитывать не только идеальные сценарии, но и возможные отклонения, улучшая ее устойчивость к непредвиденным ситуациям. В системах обнаружения вторжений (Intrusion Detection System, IDS), где истинные решения часто субъективны и зависят от контекста, шум отражает эту неопределенность, делая предсказания более реалистичными и полезными для операторов.

В реальности такие данные могут быть получены из журналов систем обнаружения вторжений, анализа сетевого трафика и баз данных реагирования на инциденты, предоставляемых организациями.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

Разработанная система поддержки принятия решений прошла комплексное тестирование на наборе данных UNSW-NB15 и синтетических данных, предназначенных для обучения модуля принятия решений, и моделирующих признаки реальных атак и принципы реагирования на инциденты. Полученные результаты подтверждают практическую применимость системы для внедрения в корпоративную инфраструктуру, для обеспечения поддержки специалистам службы безопасности в процессе анализа сетевых событий.

Модуль обнаружения угроз, реализованный на основе алгоритма XGBoost и обученный на наборе данных UNSW-NB15, демонстрирует общую точность классификации 66,07% при тестировании на 82332 событиях (рисунок 2). Взвешенные средние метрики составляют: точность (precision) 86%, полнота (recall) 66% и F1-мера 72%, что указывает на хорошую производительность для доминирующих классов атак. Однако макро-средние значения (точность 45%, полнота 62%, F1-мера 44%) показывают дисбаланс в данных и проблемы с редкими классами.

```
Модуль обнаружения угроз (XGBoost):
Accuracy: 0.6607
Отчет по классификации для Модуля обнаружения угроз:
                precision    recall  f1-score   support

        Normal       0.02      0.12      0.04       677
Reconnaissance       0.06      0.37      0.11       583
      Analysis       0.34      0.41      0.37      4089
       Fuzzers       0.84      0.51      0.64     11132
      Backdoor       0.25      0.63      0.36      6062
      Exploits       1.00      0.96      0.98     18871
           DoS       1.00      0.58      0.73     37000
       Generic       0.85      0.84      0.85      3496
     Shellcode       0.08      0.87      0.14       378
         Worms       0.09      0.89      0.17        44

      accuracy                           0.66     82332
     macro avg       0.45      0.62      0.44     82332
  weighted avg       0.86      0.66      0.72     82332

Confusion Matrix для Модуля обнаружения угроз:
[[   81   180   358    58     0     0     0     0     0]
 [   76   217   261     9     9     0     0     0    11     0]
 [  543  1051  1690   492   164     8     2    35    83    21]
 [  720  1246  1773  5708   755     0     2   415   282   231]
 [  199   476   624    35  3846     0     2    19   821    40]
 [    7    44   124   280   193 18172     1     4    27    19]
 [ 2102    20    27   158 10578     0 21383    25  2674    33]
 [   53   144   156    45    19     4     2  2937   105    31]
 [    0     5     0     3    38     0     0     2   327     3]
 [    0     0     0     1     3     0     0     0     1    39]]
```

Рис. 2. Результаты обучения и тестирования Модуля обнаружения угроз
Fig. 2. Results of training and implementation of the Threat Detection Module

После обучения и проверки Модуля принятия решений получилась модель, которая показывает умеренную способность классифицировать сценарии реагирования на угрозы информационной безопасности, и правильно определяет, как реагировать на угрозы в 67% случаев (рисунок 3). Таким образом, основываясь на полученных результатах тестирования разработанной системы поддержки принятия решений, можно заключить, что эта система позволит специалистам служб безопасности предприятий уделять особое вниманием потенциально опасным событиями, т.е., тем, которые могут иметь высокие риски и представляют угрозу для штатного функционирования предприятия. Это возможно за счет снабжения сотрудников информацией о спектре возможных действий при возникновении определенных событий.

В контексте проводимых в данной научной работе исследований, также следует указать на тот факт, что в научной литературе многие авторы подчеркивают важную роль, которую современные технологии искусственного интеллекта играют в решении задачи автоматизации процессов анализа угроз информационной безопасности, что, соответственно, подтверждает актуальность проведения исследований в этой области. Например, в научной статье [22] подчеркивается необходимость выполнения автоматизации задач, которые решают специалисты службы безопасности, с использованием искусственного интеллекта. Внедрение интеллектуальных технологий преследует цель повышения эффективности обнаружения и скорости реагирования на угрозы информационной безопасности. Основная мысль работы заключается в том, что хотя интеллектуальные технологии могут улучшить функционирование центров управления безопасностью (Security Operations Center, SOC), их применение требует человеческого мониторинга для снижения потенциальных рисков.

Отраслевые обзоры, такие как на онлайн-ресурсе CSO Online, подчеркивают необходимость автоматизации процессов анализа событий и инцидентов информационной безопасности для борьбы с растущими угрозами (52% организаций регистрируют увеличение количества угроз и инцидентов), отмечая текущий уровень автоматизации (46% значительно, 44% частично),

препятствия (39% нехватка навыков, 21% незрелость процессов) и преимущества (снижение времени реагирования и повышение точности) [23].

Точность модели решений на данных от модулей: 0.6658

Отчет по классификации на данных от модулей:

	precision	recall	f1-score	support
Analyze and block and Notify admin	0.00	0.00	0.00	563
Block and Notify admin	0.08	0.43	0.13	607
Block and fix vulnerability	0.00	0.00	0.00	2528
Block and isolate and Notify admin	0.00	0.00	0.00	1372
Fix vulnerability	0.00	0.00	0.00	1137
Full isolation and Notify admin	0.08	0.97	0.14	338
Full traffic blocking and Notify admin	0.00	0.00	0.00	1647
Ignore	1.00	0.58	0.73	37000
Investigate	1.00	0.98	0.99	18489
Isolate and block and Notify admin	0.83	0.80	0.81	7508
Limit traffic	0.34	0.91	0.49	1862
Monitor	0.44	1.00	0.61	3161
Monitor and analyze	0.00	0.00	0.00	537
Monitor traffic	0.00	0.00	0.00	800
Quarantine	0.00	0.00	0.00	38
Quarantine and delete and Notify admin	0.00	0.00	0.00	3
Restrict access	0.00	0.00	0.00	270
Restrict and monitor	0.25	0.86	0.38	4470
Scan	0.00	0.00	0.00	2
accuracy			0.67	82332
macro avg	0.21	0.34	0.23	82332
weighted avg	0.79	0.67	0.68	82332

Рис. 3. Результаты обучения и тестирования Модуля принятия решений
Fig. 3. Results of training and implementation of the Decision-making Module

В отличие от традиционных автоматизированных систем мониторинга, которые в основном участвуют в обнаружении угроз и предупреждении, предложенная система представляет собой комплексную модульную архитектуру, включающую механизмы классификации, оценки рисков, а также генерации сценариев реагирования.

Таким образом, можно заключить, что полученные результаты подтверждают эффективность разработанной системы поддержки принятия решений, позволяющей реализовать оперативное реагирование на угрозы, и формирование обоснованных решений.

ЗАКЛЮЧЕНИЕ

В результате проведенного исследования была разработана система поддержки принятия решений на основе алгоритмов машинного обучения. Особенностью системы стала ее реализация на основе модульной архитектуры, позволяющей гибко настраивать и модернизировать систему под задачи и потребности внедрения в компьютерной сети предприятия. Система может автоматически формировать сценарии реагирования на атаки, что особенно актуально в современных условиях эволюции угроз информационной безопасности. Таким образом, разработанная система позволит сотрудникам службы безопасности своевременно замечать и реагировать на события безопасности в компьютерной сети предприятия, снизить эффект и последствия влияния человеческого фактора на общую защищенность системы.

В качестве дальнейшего развития и совершенствования системы мы считаем рационально будет выполнить расширение датасетов образцами угроз и вариантами реагирования на них. Это можно реализовать с помощью интеграции системы с реальными данными SOC для обеспечения практической применимости системы в реальных условиях функционирования систем защиты информации. Также вполне обоснованным будет внедрение в архитектуру системы дополнительного модуля, который будет решать задачу объяснимого искусственного интеллекта

(SHapley Additive exPlanations, SHAP), что позволит повысить доверие специалистов к получаемым автоматизированным решениям.

Список литературы

1. Голикова А.А., Мишина Н.А. Угрозы кибербезопасности в условиях цифровизации бизнес-процессов // Актуальные проблемы и тенденции развития современной экономики: Сборник материалов Международной научно-практической конференции, Самара, 28–29 октября 2024 года. – Самара: Самарский государственный технический университет, 2024. – С. 433-437. – EDN AHCYAY.

2. Jada Irshaad, Mayayise Thembekile. The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. Data and Information Management. – 2023. – 8(2) – 100063. 10.1016/j.dim.2023.100063.

3. Santos R., Boente A., Ferreira V., Boente R., Luz D., Duarte L., Santos A., Vasconcelos G. Artificial intelligence and cybersecurity: A study of artificial intelligence in cybernetic defense // ARACÊ. – 2025. – No. 7. – P. 23155–23178. – DOI: 10.56238/arev7n5-133.

4. Mohamed N. Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms // Knowledge and Information Systems. – 2025. – Vol. 67. – No. 6969–7055. – DOI: 10.1007/s10115-025-02429-y.

5. Lysenko S. The Role of Artificial Intelligence in Cybersecurity: Automation of Protection and Detection of Threats. Economic Affairs. 2024. – 69. – 10.46852/0424-2513.1.2024.6.

6. Manoj Nair Meghna, Deshmukh Atharva, Tyagi Amit. Artificial Intelligence for Cyber Security: Current Trends and Future Challenges. – 2023. – 10.1002/9781394213948.ch5.

7. Ozkan Merve, Akin Erdal, Aslan Ömer, Kosunalp Selahattin, Iliev Teodor, Stoyanov Ivaylo. A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. IEEE Access. PP. – 2024. – 10.1109/ACCESS.2024.3355547.

8. Naik Binny, Mehta Ashir, Yagnik Hiteshri, Shah Manan. The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review. Complex & Intelligent Systems. – 2021. – 8. 10.1007/s40747-021-00494-8.

9. Akhtar Muhammad, Feng Tao. An overview of the applications of Artificial Intelligence in Cybersecurity. EAI Endorsed Transactions on Creative Technologies. – 2021. – 172218. 10.4108/eai.23-11-2021.172218.

10.Rjoub Gaith, Bentahar Jamal, Wahab Omar, Mizouni Rabeb, Song Alyssa, Cohen Robin, Otrok Hadi, Mourad Azzam, Cheriton David. A Survey on Explainable Artificial Intelligence for Cybersecurity. – 2023. – 10.48550/arXiv.2303.12942.

11.Назарова О.О. Области применения систем поддержки принятия решений // Экономика России: новые вызовы и перспективы: Сборник научных трудов Института технологий управления ФГБОУ ВО «МИРЭА - Российский технологический университет». – Москва: ООО "Издательство "Спутник+", 2022. – С. 216-226. – EDN OXQNJD.

12.Калязина Е.Г. Искусственный интеллект в системах поддержки принятия решений на примере управления проектами // International Conference GSOM Economy & Management Conference 2024, 01–05 октября 2024 года, 2024. – St. Petersburg: St. Petersburg State University, 2024. – С. 382-392.

13.Симанков В.С. Система поддержки принятия решений интеллектуального ситуационного центра для обеспечения информационной безопасности / В.С. Симанков, Л.И. Саляхова // Поведенческие теории и практика российской науки: Сборник научных статей по итогам международной научно-практической конференции, Санкт-Петербург, 26–27 февраля 2021 года. – Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2021. – С. 42-45. – EDN YTQVGL.

14.Акимов Н.Н. Информационная система поддержки принятия решений разработчиком для обеспечения компьютерной безопасности систем верхнего уровня атомных электростанций / Н.Н. Акимов, С.П. Харченко, А.Ю. Павлин // Высокие технологии атомной отрасли. Молодежь в инновационном процессе: сборник материалов XV научно-технической конференции молодых специалистов Росатома, Нижний Новгород, 15–16 сентября 2021 года. – Саров: Российский Федеральный ядерный центр - Всероссийский научно-исследовательский институт экспериментальной физики, 2021. – С. 9-14. – DOI 10.53403/9785951505033_9. – EDN BHGHLA.

15.Современные системы поддержки принятия решений и проблемы использования в них нейронных сетей / Е.И. Воеводина, Ю.М. Гуляева, Д.Е. Варахтин [и др.] // Экономика и управление: проблемы, решения. – 2023. – Т. 2, № 2(134). – С. 69-74. – DOI 10.36871/ek.up.p.r.2023.02.02.008. – EDN WTRBXL.

16.Кириллова А.Д., Вульфин А.М., Васильев В.И., Гузаиров М.Б. Интеллектуальная система поддержки принятия решений при оценке рисков нарушения информационной безопасности АСУ ТП промышленных объектов. Моделирование, оптимизация и информационные технологии. 2023; 11(4). URL: https://moitvivt.ru/ru/journal/pdf?id=1476 DOI: 10.26102/2310-6018/2023.43.4.029

17.Чупакова А.О. Разработка и обучение модели искусственной нейронной сети для создания систем поддержки принятия решений / А.О. Чупакова, С.В. Гудин, Р.Ш. Хабибулин // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. – 2020. – № 3. – С. 61-73. – DOI 10.24143/2072-9502-2020-3-61-73. – EDN IUVHKB.

18.Баранов В.В. Методические основы поддержки принятия решений при разработке систем защиты объектов информатизации / В.В. Баранов // Информационная безопасность цифровой экономики: Материалы XVIII Всероссийской научно-практической конференции (в рамках IX Пленума регионального отделения Федерального учебно-методического объединения в системе высшего образования по укрупненной группе специальностей и направлений подготовки 10.00.00 «Информационная безопасность» по Сибирскому и Дальневосточному федеральным округам (СибРОУМО)), Хабаровск, 29 июня – 01 2022 года. – Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2022. – С. 35-42. – EDN GBPTSU.

19.Kirillova A.D., Vulfin A.M., Vasilyev V.I., Guzairov M.B. Intelligent decision support system for assessing information security risks of ICS. Modeling, Optimization and Information Technology. 2023; 11(4). URL: https://moitvivt.ru/ru/journal/pdf?id=1476 DOI: 10.26102/2310-6018/2023.43.4.029.

20.Чукин А.Ю. Методика оценки защищенности сложной организационно-технической системы с внедрением системы поддержки принятия решения / А.Ю. Чукин, Н.И. Елисеев, И.М. Антоненко // Автоматизация процессов управления. – 2023. – № 1(71). – С. 51-59. – DOI 10.35752/1991-2927_2023_1_71_51. – EDN ODSPNY.

21.Moustafa N., Jill S. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set) 2015 Military Communications and Information Systems Conference (MilCIS). Canberra, ACT, pp. 1–6, 2015. DOI: 10.1109/MilCIS.2015.7348942

22.Toluwalope Ajayi, James Andrew. Automating Security Operations Centers (SOCs) with AI: Benefits and Challenges. – 2025.

23.Олтсик Дж. Обоснование автоматизации операций безопасности / Джон Олтсик // CSO. – 2022. – 3 нояб. – Режим доступа: https://www.csoonline.com/article/573997/making-the-case-for-security-operation-automation.html (дата обращения: 24.11.2025).

References

1. Golikova A.A., Mishina N.A. Cybersecurity Threats in the Context of Digital Business Processes. In Current Issues and Trends in Modern Economics Development, 433–437. Samara: Samara State Technical University, 2024.– P. 433-437. – EDN AHCYAY.

2. Jada Irshaad, Mayayise Thembekile. The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. Data and Information Management. – 2023. – 8(2) – 100063. 10.1016/j.dim.2023.100063.

3. Santos R., Boente A., Ferreira V., Boente R., Luz D., Duarte L., Santos A., Vasconcelos G. Artificial intelligence and cybersecurity: A study of artificial intelligence in cybernetic defense // ARACÊ. – 2025. – No. 7. – P. 23155–23178. – DOI: 10.56238/arev7n5-133.

4. Mohamed N. Artificial intelligence and machine learning in cybersecurity: A deep dive into state-of-the-art techniques and future paradigms // Knowledge and Information Systems. – 2025. – Vol. 67. – No. 6969–7055. – DOI: 10.1007/s10115-025-02429-y.

5. Lysenko S. The Role of Artificial Intelligence in Cybersecurity: Automation of Protection and Detection of Threats. Economic Affairs. 2024. – 69. – 10.46852/0424-2513.1.2024.6.

6. Manoj Nair Meghna, Deshmukh Atharva, Tyagi Amit. Artificial Intelligence for Cyber Security: Current Trends and Future Challenges. – 2023. – 10.1002/9781394213948.ch5.

7. Ozkan Merve, Akin Erdal, Aslan Ömer, Kosunalp Selahattin, Iliev Teodor, Stoyanov Ivaylo. A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. IEEE Access. PP. – 2024. – 10.1109/ACCESS.2024.3355547.

8. Naik Binny, Mehta Ashir, Yagnik Hiteshri, Shah Manan. The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review. Complex & Intelligent Systems. – 2021. – 8. 10.1007/s40747-021-00494-8.

9. Akhtar Muhammad, Feng Tao. An overview of the applications of Artificial Intelligence in Cybersecurity. EAI Endorsed Transactions on Creative Technologies. – 2021. – 172218. 10.4108/eai.23-11-2021.172218.

10. Rjoub Gaith, Bentahar Jamal, Wahab Omar, Mizouni Rabeb, Song Alyssa, Cohen Robin, Otrok Hadi, Mourad Azzam, Cheriton David. A Survey on Explainable Artificial Intelligence for Cybersecurity. – 2023. – 10.48550/arXiv.2303.12942.

11. Nazarova O.O. Applications of Decision Support Systems. In Russia's Economy: New Challenges and Perspectives, 216–226. Moscow: Sputnik+ Publishing, 2022. – P. 216-226. – EDN OXQNJD.

12. Kalyazina E.G. Artificial Intelligence in Decision Support Systems on the Example of Project Management. In International Conference GSOM Economy & Management Conference 2024, October 01–05, 2024. – St. Petersburg: St. Petersburg State University, 2024. – P 382–392.

13. Simankov V.S., Salyakhova L.I. System Supporting Decision-Making in an Intelligent Situational Center for Information Security. In Behavioral Theories and Practices of Russian Science, 42–45. Saint Petersburg: Saint Petersburg State University of Economics, 2021. – P. 42-45. – EDN YTQVGL.

14. Akimov N.N., Kharchenko S.P., Pavlin A.Yu. Information Support System Developer for Ensuring Computer Security of Top-Level Nuclear Power Plant Systems. In High Technologies of the Atomic Industry, 9–14. Nizhny Novgorod: Rosatom, 2021. DOI: 10.53403/9785951505033_9.

15. Voevodina E.I., Gulyaeva Y.M., Varahitin D.E. Modern Decision Support Systems and Challenges of Using Neural Networks. Economics and Management: Problems and Solutions 2 (2023): 69–74. https://doi.org/10.36871/ek.up.p.r.2023.02.02.008.

16. Kirillova A.D., Vulfing A.M., Vasilev V.I., Guzayrov M.B. Intelligent Decision Support System for Risk Assessment of Information Security of Industrial Control Systems. Modeling, Optimization and Information Technologies. – 2023. – 11, no. 4. https://doi.org/10.26102/2310-6018/2023.43.4.029.

17. Chupakova A.O., Gudin S.V., Khabibulin R.Sh. Development and Training of an Artificial Neural Network Model for Creating Decision Support Systems. Bulletin of Astrakhan State Technical University, Series Management, Computing and Informatics. – 2020. – 3. – P. 61–73. https://doi.org/10.24143/2072-9502-2020-3-61-73.

18. Baranov V.V. Methodological Foundations for Supporting Decision-Making in the Development of Information Security Systems. In Conference Proceedings. Khabarovsk: Siberian State University of Telecommunications and Informatics, 2022, 35–42.

19. Kirillova A.D., Vulfin A.M., Vasilyev V.I., Guzairov M.B. Intelligent decision support system for assessing information security risks of ICS. Modeling, Optimization and Information Technology. 2023; 11(4). URL: https://moitvivt.ru/ru/journal/pdf?id=1476 DOI: 10.26102/2310-6018/2023.43.4.029.

20. Chukin A.Yu., Eliseev N.I., Antonenko I.M. Methodology for Assessing the Security of a Complex Organizational-Technical System with the Implementation of a Decision Support System. Automation of Management Processes. 2023. – 1. – P. 51–59. https://doi.org/10.35752/1991-2927_2023_1_71_51.

21. Moustafa N., Jill S. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set) 2015 Military Communications and Information Systems Conference (MilCIS). Canberra, ACT, pp. 1–6, 2015. DOI: 10.1109/MilCIS.2015.7348942

22. Toluwalope Ajayi, James Andrew. Automating Security Operations Centers (SOCs) with AI: Benefits and Challenges. – 2025.

23. Oltsik J. Making the Case for Security Operation Automation. CSO, November 3, 2022. https://www.csoonline.com/article/573997/making-the-case-for-security-operation-automation.html

Чмыхало Данил Сергеевич, магистрант кафедры «Информационная безопасность в вычислительных системах и сетях», ФГБОУ ВО «Донской государственный технический университет» (ДГТУ), г. Ростов-на-Дону, Россия
Газизов Андрей Равильевич, кандидат педагогических наук, доцент, доцент кафедры «Информационная безопасность в вычислительных системах и сетях», ФГБОУ ВО «Донской государственный технический университет» (ДГТУ), г. Ростов-на-Дону, Россия
Легонько Ольга Леонидовна, кандидат технических наук, доцент, доцент кафедры «Информационная безопасность в вычислительных системах и сетях», ФГБОУ ВО «Донской государственный технический университет» (ДГТУ), г. Ростов-на-Дону, Россия

Чмыхало Данил Сергеевич, Master's student of the Department of Information security in computing systems and networks, Don State Technical University, Rostov-on-Don, Russia
Gazizov Andrey Ravilevich, Candidate of Pedagogical Sciences, Associate Professor, Associate Professor of the Department of Information security in computing systems and networks, Don State Technical University, Rostov-on-Don, Russia
Legonko Olga Leonidovna, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Information security in computing systems and networks, Don State Technical University, Rostov-on-Don, Russia