УДК 004.056.53 Вестник УрФО № 1(55) / 2025, с. 62–69

**Кушнир Н. В., Яцкевич Е. С.,
Власенко А. В., Копцов С. В.**

DOI: 10.14529/secur250107

ПЕРЕДОВЫЕ ПОДХОДЫ К ОЦЕНКЕ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Растущая зависимость от цифровых технологий повысила важность обеспечения безопасности объектов критической информационной инфраструктуры (КИИ), которые жизненно важны для национальной безопасности, экономической стабильности и общественной безопасности.

В данной статье рассматриваются современные подходы к оценке безопасности объектов КИИ в России, с акцентом на методологии, основанные на оценке рисков, соблюдении требований законодательства и технологиях с применением технологий искусственного интеллекта.

На основе всестороннего анализа существующих методов оценки безопасности, тематических исследований из ключевых секторов, таких как энергетика, финансы и здравоохранение, а также оценки новых тенденций, таких как искусственный интеллект (ИИ) и машинное обучение, в этом исследовании определена методика оценки защищенности КИИ с применением современных подходов и технологий.

Результаты подчеркивают необходимость интеграции передовых технологий, повышения осведомленности о безопасности, ориентированной на человека, и обеспечения соответствия нормативным требованиям для противодействия возникающим киберугрозам.

Ключевые слова: *критическая информационная инфраструктура, искусственный интеллект, оценка защищённости, киберугроза, кибератака, методика оценки.*

ADVANCED APPROACHES TO ASSESSING THE SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

The growing dependence on digital technologies has increased the importance of ensuring the security of critical information infrastructure facilities, which are vital for national security, economic stability, and public safety.

This article examines modern approaches to assessing the safety of CII facilities in Russia, with an emphasis on methodologies based on risk assessment, compliance with legal requirements and technology.

Based on a comprehensive analysis of existing security assessment methods, case studies from key sectors such as energy, finance and healthcare, as well as an assessment of new trends such as artificial intelligence (AI) and machine learning, this study defines a methodology for assessing the security of CII using modern approaches and technologies.

The results highlight the need to integrate cutting-edge technologies, raise awareness of human-centered security, and ensure regulatory compliance to counter emerging cyber threats.

Keywords: *critical information infrastructure, artificial intelligence, security assessment, cyber threat, cyber attack, assessment methodology.*

Введение

Критическая информационная инфраструктура (КИИ) представляет собой основу современного общества, охватывая системы и активы, необходимые для поддержания экономической стабильности, общественной и национальной безопасности. Эти инфраструктуры охватывают широкий спектр секторов, включая энергетику, финансы, здравоохранение, транспорт и государственные услуги. В России, растущая интеграция цифровых технологий в КИИ значительно повысила операционную эффективность, но также привела к появлению новых уязвимостей [1,2]. Киберугрозы, стихийные бедствия, инсайдерские риски и технические сбои создают серьезные проблемы для безопасности этих жизненно важных систем [3].

Растущая сложность и частота кибератак, нацеленных на объекты КИИ, подчеркивают настоятельную необходимость в надежных и адаптивных подходах к оценке безопасности. Традиционные методы, хотя и являются основополагающими, часто не учитывают динамичный и сложный характер современных угроз. Обеспечение устойчивости КИИ требует всестороннего понимания как существующих уязвимостей, так и возникающих рисков. Без эффективной оценки безопасности критически важные системы по-прежнему подвержены потенциальным сбоям [4,5].

Защита КИИ имеет первостепенное значение для обеспечения бесперебойного функционирования основных служб и сохранения общественного доверия.

Оценка защищенности объектов КИИ с помощью искусственного интеллекта

Искусственный интеллект (ИИ) все чаще используется для повышения эффективности оценки безопасности объектов критической информационной инфраструктуры (КИИ). Инструменты, основанные на ИИ, включая машинное обучение (ML) и нейронные сети, предлагают расширенные возможности для выявления уязвимостей, прогнозирования угроз и автоматизации реагирования. Эти системы анализируют огромные объемы данных для выявления аномалий, определения приоритетности рисков и предоставления

информации, пригодной для принятия мер по их устранению [6].

Например, системы обнаружения вторжений на базе искусственного интеллекта могут выявлять кибератаки и реагировать на них в режиме реального времени, в то время как инструменты поведенческой аналитики отслеживают активность пользователей для выявления внутренних угроз. Несмотря на преимущества, такие проблемы, как качество данных, техническая сложность и этические соображения, остаются. Будущие достижения, скорее всего, будут направлены на интеграцию ИИ с новыми технологиями, обеспечение понятности и противодействие враждебным атакам. Используя ИИ, организации могут применять упреждающий и адаптивный подход к защите объектов КИИ от возникающих угроз.

Уровни защищенности представляют собой гипотетические категории, которые могут обозначать различные аспекты или степени защиты системы.

Для анализа выделены следующие уровни защищенности:

Уровень 1: базовая защита, включающая стандартные меры безопасности, такие как антивирусное ПО и брандмауэры.

Уровень 2: улучшенная защита, добавляющая механизмы обнаружения вторжений и регулярные обновления безопасности.

Уровень 3: продвинутая защита, включающая шифрование данных, многофакторную аутентификацию и мониторинг безопасности в реальном времени.

Уровень 4: высокий уровень защиты с использованием машинного обучения для анализа угроз и автоматического реагирования на инциденты.

Уровень 5: максимальная защита, включающая все вышеперечисленные меры, а также проактивные стратегии, такие как симуляции атак и постоянное совершенствование системы безопасности [7,8].

Данные для анализа представлены в отчетах организаций, которые интегрировали ИИ в свои системы безопасности, такие как Ideco, Staffcop, Сбербанк и многие другие вендоры передовых информационных технологий. Зависимость защищенности представлена на рисунке 1.

Методика анализа защищенности системы с применением ИИ

Методология анализа безопасности объектов КИИ с использованием искусственного интеллекта (ИИ) предполагает структурированный подход, который объединяет качественные и количественные методы. В нем используются инструменты искусственного интеллекта, такие как машинное обучение, нейронные сети и предиктивная аналитика,

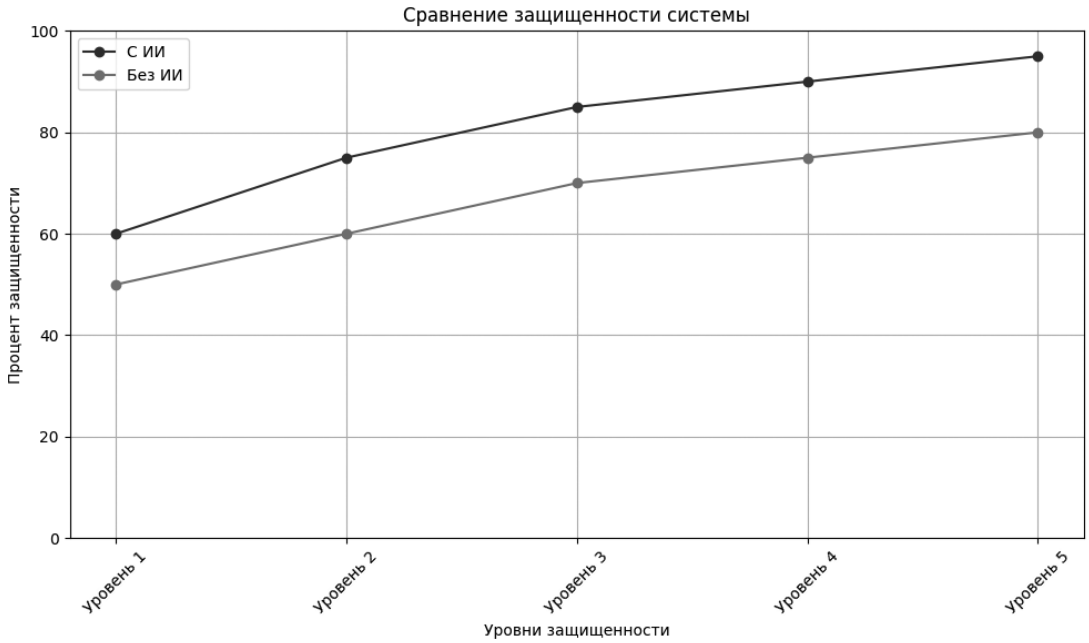

Рис. 1. Сравнения защищенности системы с применением ИИ

Таблица 1

Источники данных для анализа безопасности на основе искусственного интеллекта

Источник данных	Описание	Назначение в модели искусственного интеллекта
Журналы сетевого трафика	Журналы входящего / исходящего трафика	Обнаружение аномалий и потенциальных вторжений
Системные журналы	Журналы системных событий и ошибок	Выявление неправильных настроек или сбоев
Отчеты о сканировании уязвимостей	Результаты автоматического сканирования слабых мест	Определение приоритетности уязвимостей
Исторические данные об инцидентах	Записи прошлых кибератак и ответов	Обучение прогностическим моделям
Каналы анализа угроз	Обновления о возникающих угрозах в режиме реального времени	Усиление механизмов упреждающей защиты

для оценки уязвимостей, прогнозирования угроз и улучшения процесса принятия решений [9].

В исследовании используется гибридный подход, сочетающий в себе:

• Качественный анализ: интервью с экспертами по кибербезопасности и анализ документов для получения информации о современных методах обеспечения безопасности.

• Количественный анализ: использование алгоритмов, управляемых искусственным интеллектом, для обработки больших массивов данных для обнаружения угроз, оценки рисков и смягчения последствий.

Платформа, основанная на ИИ, фокусируется на трех основных компонентах:

1. Сбор и предварительная обработка данных.
2. Разработка и обучение модели ИИ.
3. Оценка эффективности и валидация.

Данные собираются из нескольких источников:

- Сетевые журналы: структура трафика, системные журналы и активность пользователей.
- Сканирование уязвимостей: результаты с помощью автоматизированных инструментов сканирования уязвимостей.
- Исторические данные об инцидентах: записи о прошлых кибератаках и взломах.
- Информация о внешних угрозах: данные из глобальных баз данных по кибербезопасности.

Аналитическая структура состоит из трех этапов:

Этап 1 – предварительная обработка данных.

Исходные данные очищаются и нормализуются для обеспечения совместимости с моделями искусственного интеллекта. Основные этапы предварительной обработки включают:

- Нормализация: масштабирование числовых характеристик до стандартного диапазона (например, 0-1).
- Извлечение признаков: определение релевантных признаков для анализа.
- Маркировка: присвоение меток историческим данным для контролируемого обучения (например, «нормальным» или «аномальным»).

Чтобы нормализовать функцию X до диапазона (0,1):

$$Xnormalized = \frac{X - Xmin}{Xmax - Xmin}, \qquad (1)$$

где

$Xmin$ и $Xmax$ – это минимальное и максимальные значения функции.

Этап 2 – разработка модели искусственного интеллекта.

Модели искусственного интеллекта обучены анализировать риски безопасности и уязвимости. Распространенные модели включают:

1. Контролируемое обучение: для обнаружения известных угроз (например, классификационных моделей, таких как случайный лес или машины опорных векторов).

Таблица 2

Модели искусственного интеллекта и их приложения

Тип модели	Алгоритм	Приложения
Контролируемое обучение	Случайный лес	Классифицирует сетевой трафик как нормальный / аномальный
Неконтролируемое обучение	DBSCAN	Обнаруживает отклонения в поведении системы
Обучение с подкреплением	Q-Learning	Оптимизация автоматического реагирования на инциденты
Нейронные сети	Сверточные нейронные сети (CNN)	Анализ сигнатур вредоносных программ на основе изображений

2. Обучение без учителя: для выявления неизвестных угроз (например, алгоритмов кластеризации, таких как k-средние значения).
3. Обучение с подкреплением: для оптимизации стратегий реагирования на инциденты.

Аномалии обнаруживаются на основе отклонений от среднего значения:

$$P(X) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(X-\mu)^2}{2\sigma^2}}, \quad (2)$$

где

$P(X)$ – вероятность наблюдения значения X.

μ – среднее значение набора данных.

σ^2 – дисперсия набора данных.

Если $P(X) <$ пороговое значение, наблюдение помечается как аномальное.

Этап 3 – оценка эффективности.

Производительность моделей искусственного интеллекта оценивается с помощью таких показателей, как точность, прецизионность, отзыв и оценка F1. Кроме того, для визуализации результатов используются матрицы путаницы.

Истинные положительные результаты (True Positives, TP): случаи, когда модель правильно предсказывает положительный класс.

Истинные негативы (True Negatives, TN): случаи, когда модель правильно предсказывает отрицательный класс.

Ложноположительные результаты (FP): случаи, когда модель неверно предсказывает положительный класс (ошибка I типа).

Ложные отрицательные результаты (FN): случаи, когда модель неверно предсказывает отрицательный класс (ошибка II типа).

Точность: доля правильно идентифицированных аномалий среди всех прогнозируемых аномалий.

$$\text{Точность} = \frac{TP}{TP+FP}. \quad (3)$$

Отзыв: доля правильно идентифицированных аномалий среди всех фактических аномалий.

$$\text{Отзыв} = \frac{TP}{TP+FN}. \quad (4)$$

С помощью этих показателей оценивается эффективность предлагаемой модели с применением искусственного интеллекта.

Эта методология обеспечивает систематический способ анализа безопасности объектов КИИ с использованием искусственного интеллекта. Используя передовые алгоритмы и постоянный мониторинг, организации могут достичь высокого уровня защиты от возникающих киберугроз [10].

Таблица 3

Матрица путаницы для оценки модели искусственного интеллекта

Фактический/прогнозируемый результат	Нормальный	Аномальный
Нормальный	Истинно отрицательный (TN)	Ложноположительный (FP)
Аномальный	Ложноотрицательный (FN)	Истинно положительный (TP)

Таблица 4

Ключевые этапы методологии

Шаг	Описание	Результат
Сбор данных	Сбор сетевых журналов, сканирований уязвимостей и т.д.	Полный набор данных для обучения ИИ
Предварительная обработка данных	Нормализация и маркировка данных	Очистка и структурирование данных для анализа
Разработка модели ИИ	Обучение моделей под наблюдением / без присмотра	Обученная модель для обнаружения угроз
Оценка производительности	Оценивайте, используя такие показатели, как точность и отзыв,	Валидированная модель с высокой точностью
Соблюдение этических норм	Устраняет проблемы конфиденциальности, предвзятости и объяснимости	Этически обоснованная и прозрачная модель
Развертывание и валидация	Тестируйте модель в реальных сценариях	Функциональный инструмент искусственного интеллекта для обеспечения безопасности КИИ

Заключение

Разработанная методология можем применяться для оценки защищенности объектов критической информационной инфраструктуры и является актуальной для применяемых технологий в 2025 году.

Интеграция технологий искусственного интеллекта является передовой для большинства организаций в России, поэтому технологическая база во многих случаях не требует дополнительных надстроек для интеграции разработанной методики, в связи с чем результат существующей разработки имеет высокий потенциал для внедрения.

Литература

1. Обласов А. А. Организация и технология защиты конфиденциальной информации в информационных системах: методическое пособие для студентов. — М.: Ridero, 2020. — 173 с.

2. Степаненко С. И. ГосСОПКА в области критической информационной инфраструктуры Российской Федерации / С. И. Степаненко // The World of Science Without Borders, 11 февраля 2022 года, 2022. – Р. 348-350. – EDN RQKGRV.

3. Колтунова Т. В. Правовые аспекты обеспечения информационной безопасности в критической информационной инфраструктуре / Т. В. Колтунова, Н. Л. Колтунов // Евразийский юридический журнал. – 2022. – № 3(166). – С. 413-416. – EDN GBXTYW.

4. Максимова Е. А. Проактивное Управление информационной безопасностью субъектов критической информационной инфраструктуры как сложных организационных систем с динамически изменяющейся структурой / Е. А. Максимова, М. В. Буйневич, А. В. Шестаков // Вестник Воронежского института МВД России. – 2023. – № 2. – С. 49-59. – EDN CWISSD.

5. Долженков С. С. Оптимизация системы менеджмента информационной безопасности объектов критической информационной инфраструктуры / С. С. Долженков // Студенческая наука для развития информационного общества: Материалы XУ Всероссийской научно-технической конференции с приглашением зарубежных ученых, Ставрополь, 28 ноября 2023 года. – Ставрополь: Северо-Кавказский федеральный университет, 2024. – С. 124-130. – EDN EYGAVD.

6. Фисун В. В. О необходимости интеллектуализации процессов управления информационной безопасностью на объектах критической информационной инфраструктуры / В. В. Фисун // Информационная безопасность - актуальная проблема современности. Совершенствование образовательных технологий подготовки специалистов в области информационной безопасности. – 2018. – № 1(9). – С. 255-257. – EDN JEGHAR.

7. Иконников С. Е. Создание системы защиты и автоматизация информационной безопасности на объектах критической информационной инфраструктуры / С. Е. Иконников // Интеллектуальные транспортные системы: Материалы III Международной научно-практической конференции, Москва, 30 мая 2024 года. – Москва: Российский университет транспорта (МИИТ), 2024. – С. 575-578. – DOI 10.30932/9785002446094-2024-575-578. – EDN RVIGBA.

8. Методика обеспечения устойчивости функционирования критической информационной инфраструктуры в условиях информационных воздействий / С. М. Климов, С. В. Поликарпов, Б. С. Рыжов [и др.] // Вопросы кибербезопасности. – 2019. – № 6(34). – С. 37-48. – DOI 10.21681/2311-3456-2019-6-37-48. – EDN ANVHWE.

9. Смирнов Г. Е. Актуальные вопросы развития теории и практики аудита информационной безопасности объектов критической информационной инфраструктуры / Г. Е. Смирнов, С. И. Макаренко // Проблемы комплексной безопасности Каспийского макрорегиона: Сборник научных статей по материалам международной научно-практической конференции, Астрахань, 28–29 октября 2021 года / Под общей редакцией А.П. Романовой, Д.А. Черничкина. – Астрахань: Астраханский государственный университет, Издательский дом "Астраханский университет", 2021. – С. 148-157. – EDN MSQRDC.

10. Воеводин В. А. О проблеме оценивания устойчивости функционирования объектов критической информационной инфраструктуры для условий воздействия угроз информационной безопасности / В. А. Воеводин // Радиоэлектронные устройства и системы для инфокоммуникационных технологий" ("РЭУС-ИТ 2024"): Доклады Всероссийской конференции, посвященной Дню радио, Москва, 31 мая 2024 года. – Москва: Российское научно-техническое общество радиотехники, электроники и связи им. А.С. Попова, 2024. – С. 299-304. – EDN UPBBWH.

References

1. Oblasov A. A. Organizatsiya i tekhnologiya zashchity konfidentsial'noy informatsii v informatsionnykh sistemakh: metodicheskoe posobie dlya studentov . — M.: Ridero, 2020. — 173 s.

2. Stepanenko S. I. GosSOPKA v oblasti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii / S. I. Stepanenko // The World of Science Without Borders, 11 fevralya 2022 goda, 2022. – P. 348-350. – EDN RQKGRV.

3. Koltunova T. V. Pravovye aspekty obespecheniya informatsionnoy bezopasnosti v kriticheskoy informatsionnoy infrastrukture / T. V. Koltunova, N. L. Koltunov // Evraziyskiy yuridicheskiy zhurnal. – 2022. – № 3(166). – S. 413-416. – EDN GBXTYW.

4. Maksimova E. A. Proaktivnoe Upravlenie informatsionnoy bezopasnost'yu sub"ektov kriticheskoy informatsionnoy infrastruktury kak slozhnykh organizatsionnykh sistem s dinamicheski izmenyayushcheysya strukturoy / E. A. Maksimova, M. V. Buynevich, A. V. Shestakov // Vestnik Voronezhskogo instituta MVD Rossii. – 2023. – № 2. – S. 49-59. – EDN CWISSD.

5. Dolzhenkov S. S. Optimizatsiya sistemy menedzhmenta informatsionnoy bezopasnosti ob"ektov kriticheskoy informatsionnoy infrastruktury / S. S. Dolzhenkov // Studencheskaya nauka dlya razvitiya informatsionnogo obshchestva: Materialy KhU Vserossiyskoy nauchno-tekhnicheskoy konferentsii s priglasheniem zarubezhnykh uchenykh, Stavropol', 28 noyabrya 2023 goda. – Stavropol': Severo-Kavkazskiy federal'nyy universitet, 2024. – S. 124-130. – EDN EYGAVD.

6. Fisun V. V. O neobkhodimosti intellektualizatsii protsessov upravleniya informatsionnoy bezopasnost'yu na ob"ektakh kriticheskoy informatsionnoy infrastruktury / V. V. Fisun // Informatsionnaya bezopasnost' - aktual'naya problema sovremennosti. Sovershenstvovanie obrazovatel'nykh tekhnologiy podgotovki spetsialistov v oblasti informatsionnoy bezopasnosti. – 2018. – № 1(9). – S. 255-257. – EDN JEGHAR.

7. Ikonnikov S. E. Sozdanie sistemy zashchity i avtomatizatsiya informatsionnoy bezopasnosti na ob"ektakh kriticheskoy informatsionnoy infrastruktury / S. E. Ikonnikov // Intellektual'nye transportnye sistemy: Materialy III Mezhdunarodnoy nauchno-prakticheskoy konferentsii, Moskva, 30 maya 2024 goda. – Moskva: Rossiyskiy universitet transporta (MIIT), 2024. – S. 575-578. – DOI 10.30932/9785002446094-2024-575-578. – EDN RVIGBA.

8. Metodika obespecheniya ustoychivosti funktsionirovaniya kriticheskoy informatsionnoy infrastruktury v usloviyakh informatsionnykh vozdeystviy / S. M. Klimov, S. V. Polikarpov, B. S. Ryzhov [i dr.] // Voprosy kiberbezopasnosti. – 2019. – № 6(34). – S. 37-48. – DOI 10.21681/2311-3456-2019-6-37-48. – EDN ANVHWE.

9. Smirnov G. E. Aktual'nye voprosy razvitiya teorii i praktiki audita informatsionnoy bezopasnosti ob"ektov kriticheskoy informatsionnoy infrastruktury / G. E. Smirnov, S. I. Makarenko // Problemy kompleksnoy bezopasnosti Kaspiyskogo makroregiona: Sbornik nauchnykh statey po materialam mezhdunarodnoy nauchno-prakticheskoy konferentsii, Astrakhan', 28–29 oktyabrya 2021 goda / Pod obshchey redaktsiey A.P. Romanovoy, D.A. Chernichkina. – Astrakhan': Astrakhanskiy gosudarstvennyy universitet, Izdatel'skiy dom "Astrakhanskiy universitet", 2021. – S. 148-157. – EDN MSQRDC.

10. Voevodin V. A. O probleme otsenivaniya ustoychivosti funktsionirovaniya ob"ektov kriticheskoy informatsionnoy infrastruktury dlya usloviy vozdeystviya ugroz informatsionnoy bezopasnosti / V. A. Voevodin // Radioelektronnye ustroystva i sistemy dlya infokommunikatsionnykh tekhnologiy" ("REUS-IT 2024"): Doklady Vserossiyskoy konferentsii, posvyashchennoy Dnyu radio, Moskva, 31 maya 2024 goda. – Moskva: Rossiyskoe nauchno-tekhnicheskoe obshchestvo radiotekhniki, elektroniki i svyazi im. A.S. Popova, 2024. – S. 299-304. – EDN UPBBWH.

КУШНИР Надежда Владимировна, старший преподаватель кафедры информационных систем и программирования федерального государственного бюджетного образовательного учреждения высшего образования «Кубанский государственный технологический университет». 350072, г. Краснодар, ул. Московская, д. 2. E-mail: kushnir.06@mail.ru

ЯЦКЕВИЧ Евгений Сергеевич, магистрант 2 курса федерального государственного бюджетного образовательного учреждения высшего образования «Кубанский государственный технологический университет». 350072, г. Краснодар, ул. Московская, д. 2. E-mail: es_yatskevich@internet.ru

ВЛАСЕНКО Александра Владимировна, кандидат технических наук, доцент, профессор кафедры информационной безопасности Краснодарского университета МВД России. 350005, г. Краснодар, ул. Ярославская 128. E-mail: alex_vlasenko@list.ru

КОПЦОВ Сергей Васильевич, кандидат социологических наук, полковник полиции, старший преподаватель кафедры информационной безопасности Краснодарского университета МВД России. 350005, г. Краснодар, ул. Ярославская 128. E-mail: Serega.kchr@yandex.ru

KUSHNIR Nadezhda Vladimirovna, Senior Lecturer at the Department of Information Systems and Programming of the Federal State Budgetary Educational Institution of Higher Education «Kuban State Technological University». 2 Moskovskaya St., Krasnodar, 350072. E-mail: kushnir.06@mail.ru

YATSKEVICH Evgeny Sergeevich, 2nd year Master's student at the Federal State Budgetary Educational Institution of Higher Education «Kuban State Technological University». 2 Moskovskaya St., Krasnodar, 350072. E-mail: es_yatskevich@internet.ru

VLASENKO Alexandra Vladimirovna, Candidate of Technical Sciences, Associate Professor, Professor of the Department of Information Security at the Krasnodar University of the Ministry of Internal Affairs of Russia. 128 Yaroslavskaya St., Krasnodar, 350005. E-mail: alex_vlasenko@list.ru

KOPTSOV Sergey Vasilyevich, Candidate of Sociological Sciences, Police Colonel, Senior Lecturer at the Department of Information Security of the Krasnodar University of the Ministry of Internal Affairs of Russia. 128 Yaroslavskaya St., Krasnodar, 350005. E-mail: Serega.kchr@yandex.ru