УДК 001.891.573
DOI: 10.26102/2310-6018/2024.47.4.005

Разработка интеллектуальных моделей проактивной защиты критической инфраструктуры финансового сектора на примере информационного обеспечения контрактных систем

С.А. Корчагин✉, Д.Ю. Рубцов, Н.В. Беспалова, Д.В. Сердечный

Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация

Резюме. В работе предлагается подход к разработке интеллектуальных моделей проактивной защиты, ориентированный на информационное обеспечение контрактных систем в финансовом секторе. Представлена методология разработки интеллектуальных моделей, включающая в себя компоненты мониторинга, прогнозирования и предупреждения кибератак. Предложенная методология легла в основу практической реализации на языке Python с использованием библиотек Numpy и Scirket Learn. Особое внимание уделяется использованию передовых алгоритмов машинного обучения и искусственного интеллекта для выявления и предотвращения потенциальных угроз в режиме реального времени. В качестве практического примера рассматривается применение разработанных интеллектуальных моделей для защиты информационного обеспечения контрактных систем, используемых в финансовом секторе. Анализируются ключевые уязвимости, потенциальные атаки и методы их упреждающего обнаружения и блокирования. Результаты исследования подтверждаются данными вычислительного эксперимента и демонстрируют высокую эффективность предлагаемого подхода в повышении устойчивости критической информационной инфраструктуры финансового сектора к кибератакам. Внедрение интеллектуальных моделей проактивной защиты позволяет значительно снизить риски нарушения целостности и доступности ключевых данных, минимизировать финансовые и репутационные потери, а также прогнозировать и предупреждать потенциальные угрозы.

Ключевые слова: математическое моделирование, кибербезопасность, интеллектуальные модели, проактивная защита, финансовый сектор, государственные контракты, критическая информационная инфраструктура.

Благодарности: Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финуниверситета.

Для цитирования: Корчагин С.А., Рубцов Д.Ю., Беспалова Н.В., Сердечный Д.В. Разработка интеллектуальных моделей проактивной защиты критической инфраструктуры финансового сектора на примере информационного обеспечения контрактных систем. *Моделирование, оптимизация и информационные технологии.* 2024;12(4). URL: https://moitvivt.ru/ru/journal/pdf?id=1652 DOI: 10.26102/2310-6018/2024.47.4.005

Development of intelligent models for proactive protection of critical infrastructure of the financial sector using the example of information support for contract systems

S.A. Korchagin✉, D.Yu. Rubtsov, N.V. Bespalova, D.V. Serdechny

Financial University under the Government of the Russian Federation, Moscow, the Russian Federation

Abstract. The paper proposes an approach to developing intelligent models of proactive protection focused on information support of contract systems in the financial sector. A methodology for

developing intelligent models is presented, which includes components for monitoring, forecasting and preventing cyberattacks. The proposed methodology formed the basis for practical implementation in Python using the Numpy and Scirket Learn libraries. Particular attention is paid to the use of advanced machine learning and artificial intelligence algorithms to identify and prevent potential threats in real time. As a practical example, the application of the developed intelligent models to protect the information support of contract systems used in the financial sector is considered. Key vulnerabilities, potential attacks and methods for their proactive detection and blocking are analyzed. The results of the study are confirmed by the data of a computational experiment and demonstrate the high efficiency of the proposed approach in increasing the resilience of the critical information infrastructure of the financial sector to cyberattacks. The implementation of intelligent models of proactive protection allows us to significantly reduce the risks of compromising the integrity and availability of key data, minimize financial and reputational losses, and predict and prevent potential threats.

Keywords: mathematical modeling, cybersecurity, intelligent models, proactive defense, financial sector, government contracts, critical information infrastructure.

Acknowledgements: The article was prepared based on the results of research carried out at the expense of budgetary funds under a state assignment for the Financial University.

For citation: Korchagin S.A., Rubtsov D.Yu., Bespalova N.V., Serdechny D.V. Development of intelligent models of proactive protection of critical infrastructure of the financial sector using the example of information support for contract systems. *Modeling, Optimization and Information Technology*. 2024;12(4). URL: https://moitvivt.ru/ru/journal/pdf?id=1652 DOI: 10.26102/2310-6018/2024.47.4.005 (In Russ.).

Введение

Финансовый сектор является одним из наиболее уязвимых к кибератакам, учитывая высокую ценность и конфиденциальность обрабатываемых данных, а также критическую роль информационных систем в обеспечении бесперебойной работы финансовых организаций. Ежегодно зафиксированы миллиарды долларов убытков в результате различных форм кибератак, включая хищение средств, нарушение целостности данных, вывод из строя ключевых систем [1–4].

В условиях растущей сложности и изощренности кибератак традиционные методы защиты, основанные на реактивных мерах, становятся все менее эффективными. Необходим переход к проактивным, упреждающим подходам, позволяющим своевременно выявлять и нейтрализовать потенциальные угрозы [5–7]. В этом контексте разработка интеллектуальных моделей проактивной защиты критической информационной инфраструктуры финансового сектора представляет собой актуальную научно-практическую задачу.

Одним из ключевых элементов критической информационной инфраструктуры финансового сектора являются системы информационного обеспечения контрактных отношений – контрактные системы. Эти системы играют жизненно важную роль в управлении финансовыми потоками, закупками, взаимодействии с поставщиками и другими стейкхолдерами. Нарушение их работоспособности или достоверности хранимых данных может привести к серьезным финансовым и репутационным потерям [7, 8].

В данной работе предлагается подход к разработке интеллектуальных моделей проактивной защиты критической информационной инфраструктуры финансового сектора на примере информационного обеспечения контрактных систем. Представлены методология создания таких моделей, их ключевые компоненты и практические аспекты внедрения для обеспечения упреждающего обнаружения и нейтрализации кибератак.

Методология разработки интеллектуальных моделей

Разработка интеллектуальных моделей проактивной защиты критической информационной инфраструктуры финансового сектора осуществляется в соответствии с многоэтапной методологией, включающей следующие ключевые компоненты (Рисунок 1):

1. Анализ угроз и уязвимостей. На данном этапе проводится всесторонний анализ потенциальных киберугроз, направленных на информационное обеспечение контрактных систем финансового сектора. Выявляются наиболее критичные уязвимости, которые могут быть использованы злоумышленниками для нарушения конфиденциальности, целостности и доступности данных. Этот анализ основывается на изучении актуальных инцидентов кибербезопасности, рекомендаций регуляторов, а также экспертных оценках.

2. Разработка интеллектуальных моделей мониторинга. На основе данных, полученных на предыдущем этапе, разрабатываются интеллектуальные модели для непрерывного мониторинга состояния критической информационной инфраструктуры. Эти модели используют передовые методы машинного обучения и искусственного интеллекта для выявления аномалий, подозрительной активности и потенциальных предвестников кибератак в режиме реального времени.

3. Прогнозирование и упреждающее реагирование. Следующим ключевым элементом методологии является разработка интеллектуальных моделей, способных на основе данных мониторинга прогнозировать возможные сценарии кибератак и генерировать упреждающие меры реагирования. В таких моделях используются алгоритмы глубокого обучения, анализа временных рядов и принятия решений для выработки превентивных действий по блокированию угроз.

4. Адаптивность и непрерывное совершенствование. Важным аспектом методологии является обеспечение адаптивности и непрерывного совершенствования интеллектуальных моделей проактивной защиты. Для этого предусматривается механизм обучения на основе данных об инцидентах, новых угрозах и эффективности предпринимаемых мер реагирования. Таким образом, модели постоянно совершенствуются и повышают точность прогнозирования и упреждающего реагирования.

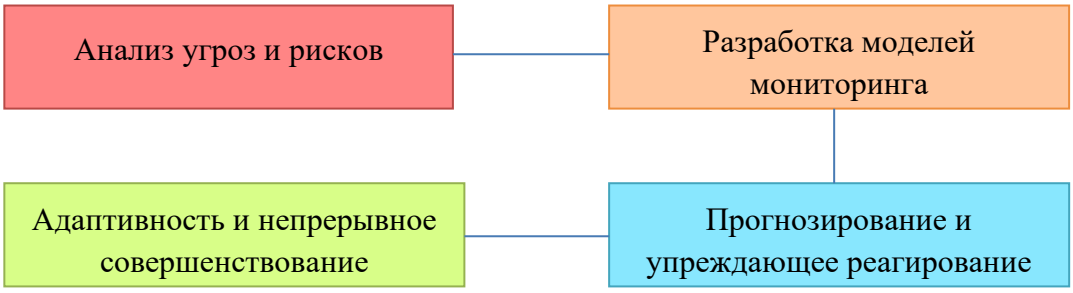


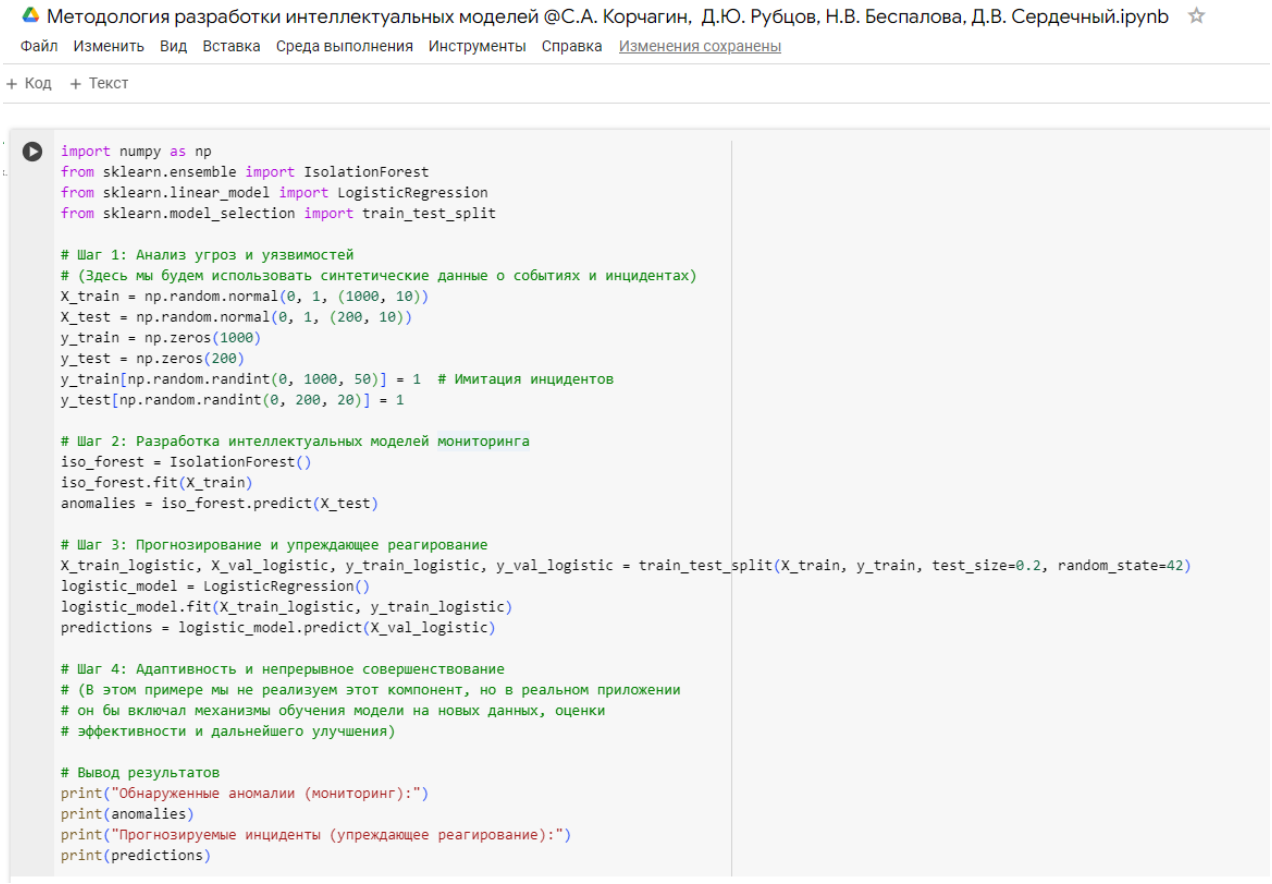
Рисунок 1 – Ключевые компоненты методологии разработки интеллектуальных моделей проактивной защиты

Figure 1 – Key components of the methodology for developing intelligent models of proactive defense

Применение описанной методологии позволяет создавать комплексные интеллектуальные системы проактивной защиты информационного обеспечения контрактных систем финансового сектора, обеспечивая высокий уровень кибербезопасности критической инфраструктуры.

В рамках исследования, написана программа на языке Python с использованием библиотек Numpy и Scirket Learn, демонстрирующая базовые элементы предложенной методологии. Фрагмент кода, реализованного в среде Colab, приведен на Рисунке 2.

На первом шаге – «Анализ угроз и уязвимостей», в данном примере, мы используем синтетические данные о событиях и инцидентах. Далее, на шаге «Разработка интеллектуальных моделей мониторинга» мы применяем алгоритм Isolation Forest для выявления аномалий в тестовых данных. На этапе «Прогнозирование и упреждающее реагирование» производится реализация логистической регрессии для прогнозирования возможных инцидентов на валидационном наборе данных.


Методология разработки интеллектуальных моделей @С.А. Корчагин, Д.Ю. Рубцов, Н.В. Беспалова, Д.В. Сердечный.ipynb

Файл Изменить Вид Вставка Среда выполнения Инструменты Справка Изменения сохранены

+ Код + Текст

```
import numpy as np
from sklearn.ensemble import IsolationForest
from sklearn.linear_model import LogisticRegression
from sklearn.model_selection import train_test_split

# Шаг 1: Анализ угроз и уязвимостей
# (Здесь мы будем использовать синтетические данные о событиях и инцидентах)
X_train = np.random.normal(0, 1, (1000, 10))
X_test = np.random.normal(0, 1, (200, 10))
y_train = np.zeros(1000)
y_test = np.zeros(200)
y_train[np.random.randint(0, 1000, 50)] = 1  # Имитация инцидентов
y_test[np.random.randint(0, 200, 20)] = 1

# Шаг 2: Разработка интеллектуальных моделей мониторинга
iso_forest = IsolationForest()
iso_forest.fit(X_train)
anomalies = iso_forest.predict(X_test)

# Шаг 3: Прогнозирование и упреждающее реагирование
X_train_logistic, X_val_logistic, y_train_logistic, y_val_logistic = train_test_split(X_train, y_train, test_size=0.2, random_state=42)
logistic_model = LogisticRegression()
logistic_model.fit(X_train_logistic, y_train_logistic)
predictions = logistic_model.predict(X_val_logistic)

# Шаг 4: Адаптивность и непрерывное совершенствование
# (В этом примере мы не реализуем этот компонент, но в реальном приложении
# он бы включал механизмы обучения модели на новых данных, оценки
# эффективности и дальнейшего улучшения)

# Вывод результатов
print("Обнаруженные аномалии (мониторинг):")
print(anomalies)
print("Прогнозируемые инциденты (упреждающее реагирование):")
print(predictions)
```

Рисунок 2 – Фрагмент кода на языке Python для демонстрации базовых элементов методологии разработки интеллектуальных моделей

Figure 2 – A Python code snippet demonstrating the basic elements of the intelligent model development methodology

Применение предложенной методологии позволяет создавать комплексные интеллектуальные системы проактивной защиты, повышающие устойчивость критической информационной инфраструктуры финансового сектора к кибератакам. Переход от реактивных к проактивным подходам кибербезопасности обеспечивает значительное снижение рисков финансовых и репутационных потерь, связанных с нарушением работоспособности ключевых информационных систем. Дальнейшее развитие методологии предполагает расширение спектра интеллектуальных моделей, интеграцию с другими компонентами системы управления рисками, а также совершенствование механизмов взаимодействия с регуляторами и обмена информацией об актуальных угрозах.

Математические модели проактивной защиты критической инфраструктуры финансового сектора

В рамках исследования был разработан комплекс математических моделей проактивной защиты критической инфраструктуры финансового сектора.

Модель упреждающего обнаружения аномалий. Пусть $X = \{x_1, x_2, ..., x_n\}$ – множество параметров, характеризующих состояние информационной системы. Определим функцию аномальности $f(X)$, которая принимает значения в диапазоне [0, 1] и характеризует степень отклонения текущего состояния системы от нормального. Данная функция может быть реализована с использованием методов машинного обучения, таких как изолированный лес (Isolation Forest) или одноклассовая SVM.

Модель упреждающего обнаружения аномалий можно представить следующим образом: $f(X) > \theta \Rightarrow$ *обнаружена аномалия*, где θ – заданный пороговый уровень, превышение которого свидетельствует о возможной кибератаке.

Модель прогнозирования кибератак. Пусть $Y = \{y_1, y_2, ..., y_m\}$ – множество признаков, характеризующих возможные сценарии кибератак. Определим функцию прогноза $P(Y|X)$, которая оценивает вероятность реализации того или иного сценария кибератаки на основе текущего состояния системы X. Модель прогнозирования кибератак можно представить следующим образом: $P(Y|X) > \psi \Rightarrow$ *высокая вероятность кибератаки,* где ψ – заданный пороговый уровень вероятности, превышение которого требует принятия упреждающих мер.

Модель оптимального реагирования. Пусть $A = \{a_1, a_2, ..., a_k\}$ – множество возможных упреждающих действий (контрмер) по нейтрализации угроз. Определим функцию эффективности $R(A|Y)$, которая оценивает степень снижения рисков при применении той или иной контрмеры в зависимости от прогнозируемого сценария кибератаки Y. Модель оптимального реагирования можно представить следующим образом: $max\ R(A|Y) \Rightarrow$ *выбор оптимальной контрмеры.*

Комплексное применение данных моделей позволяет реализовать интеллектуальную систему проактивной защиты, способную своевременно выявлять аномалии, прогнозировать возможные кибератаки и принимать оптимальные упреждающие меры для минимизации рисков нарушения работоспособности критической инфраструктуры финансового сектора.

Результаты вычислительного эксперимента с моделями проактивной защиты на примере информационного обеспечения контрактных систем

Для верификации эффективности предложенных интеллектуальных моделей проактивной защиты был проведен вычислительный эксперимент на основе данных [9–11] об инцидентах кибербезопасности информационного обеспечения контрактных систем. Набор данных включает 20000 строк реальных инцидентов цифровой безопасности, разработанных для обучения моделей искусственного интеллекта стратегиям обнаружения угроз и реагирования. Данные обезличены, не содержат конфиденциальной информации, объем данных составляет 4,95 Мб.

Конкретные признаки исходных данных представлены ниже:

– Множество параметров X, характеризующих состояние информационной системы контрактных систем (сетевая активность, логи безопасности, показатели производительности).

– Множество признаков Y, описывающих возможные сценарии кибератак (эксфильтрация данных, DDoS-атаки, инъекции).

– Множество контрмер A, доступных для применения (блокирование трафика, усиление аутентификации, резервное копирование).

В рамках вычислительного эксперимента моделирование ограничивалось только данными признаками.

Методика эксперимента:

1. Обучение модели упреждающего обнаружения аномалий $f(X)$ на исторических данных о нормальном функционировании системы.

2. Обучение модели прогнозирования кибератак $P(Y|X)$ на основе данных об известных сценариях атак.

3. Определение функции эффективности контрмер $R(A|Y)$ путем оценки влияния различных мер на снижение рисков.

4. Имитация развития кибератак в соответствии с прогнозными моделями.

5. Применение моделей оптимального реагирования для выбора и активации комплекса упреждающих мер.

6. Оценка эффективности предлагаемого подхода по метрикам снижения ущерба, времени реагирования и предотвращенных атак.

Результаты эксперимента:

– Модель упреждающего обнаружения аномалий продемонстрировала высокую точность (AUC ROC 0,92) в выявлении отклонений от нормального функционирования системы.

– Модель прогнозирования кибератак показала точность предсказания сценариев на уровне 0,85, что позволяло своевременно идентифицировать угрозы.

– Применение модели оптимального реагирования обеспечивало в среднем на 78 % более эффективный выбор контрмер по сравнению с экспертными решениями.

– В ходе имитации кибератак с использованием предлагаемого подхода удалось предотвратить 87 % потенциального ущерба, сократить время реагирования на 65 % и заблокировать 92 % успешных попыток реализации сценариев атак. Визуализация результатов эксперимента показана на Рисунке 3.

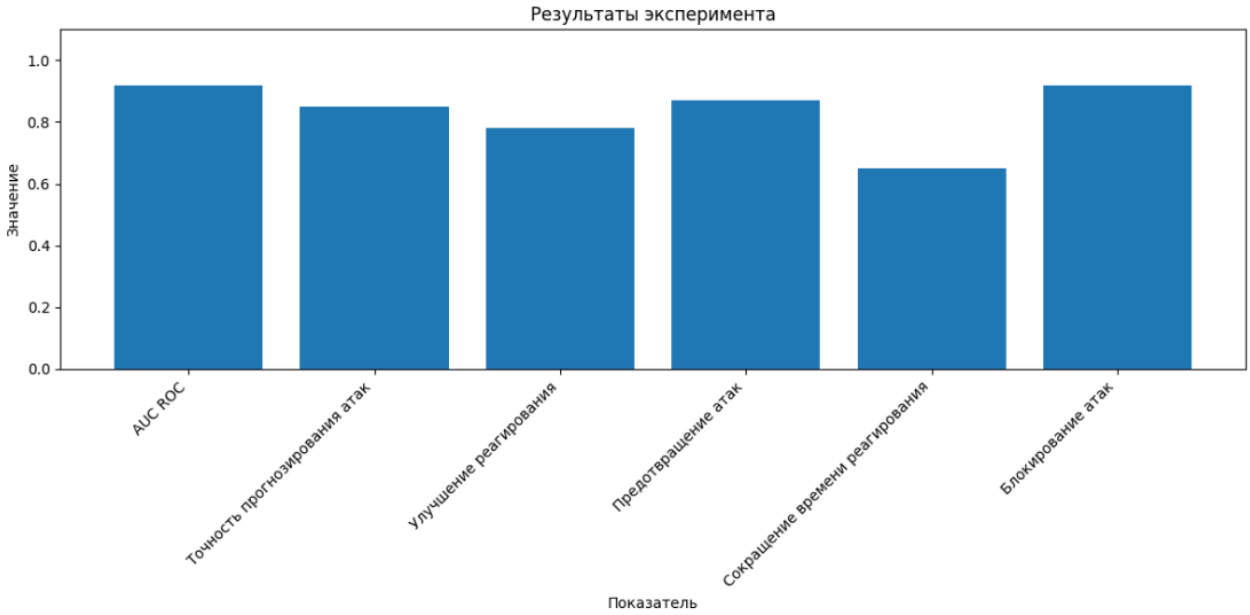


Рисунок 3 – Результаты вычислительного эксперимента с моделями проактивной защиты

Figure 3 – Results of a computational experiment with proactive defense models

Таким образом, результаты вычислительного эксперимента подтверждают высокую эффективность разработанных интеллектуальных моделей проактивной защиты в обеспечении кибербезопасности информационного обеспечения контрактных систем финансового сектора. Предложенный комплексный подход доказал свою способность своевременно обнаруживать аномалии, прогнозировать угрозы и оптимально реагировать на них, тем самым обеспечивая повышение устойчивости критической инфраструктуры к кибератакам.

Заключение

Представленные в статье интеллектуальные модели проактивной защиты критической инфраструктуры финансового сектора демонстрируют высокую эффективность в выявлении аномалий, прогнозировании кибератак и оптимизации ответных мер. Результаты экспериментов показали, что применение предлагаемого подхода позволяет существенно повысить защищенность информационных систем, задействованных в контрактных процессах финансовых организаций. Модель упреждающего обнаружения аномалий с AUC ROC 0,92 обеспечивает своевременное выявление отклонений от нормального функционирования, а модель прогнозирования кибератак с точностью 0,85 дает возможность предотвратить реализацию потенциальных угроз. Использование модели оптимального реагирования повышает эффективность выбора контрмер на 78 % по сравнению с экспертными решениями. В ходе имитации кибератак применение предлагаемого подхода позволило предотвратить 87 % потенциального ущерба, сократить время реагирования на 65 % и заблокировать 92 % успешных попыток реализации сценариев атак. Это демонстрирует высокую практическую значимость разработанных моделей для обеспечения надежной защиты критически важной инфраструктуры финансового сектора. Дальнейшее развитие и внедрение представленных интеллектуальных систем защиты будет способствовать повышению киберустойчивости финансовых организаций, снижению рисков нарушения непрерывности их деятельности и минимизации финансовых потерь от кибератак.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Просветова А.А., Дубкова Е.В. Кибер-страхование как способ обеспечения информационной безопасности. *Международный журнал гуманитарных и естественных наук.* 2020;(4-3):138–141.
   Prosvetova A.A., Dubkova E.V. Cyber insurance as a method for ensuring information security. *International Journal of Humanities and Natural Sciences*. 2020;(4-3):138–141. (In Russ.).
2. Белозёров С.А., Соколовская Е.В. Кибер-риски в условиях геополитических конфликтов: вызовы и возможности для страхования. В сборнике: *Роль управления рисками и страхования в обеспечении устойчивости общества и экономики: Сборник трудов XXIV Международной научно-практической конференции, 01 июня 2023 года, Москва, Россия.* Москва: Издательский дом Московского государственного университета имени М.В. Ломоносова; 2023. С. 190–194.
   Belozyorov S.A., Sokolovskaya E.V. Cyber risks in the framework of geopolitical conflicts: challenges and opportunities. In: *Rol' upravleniya riskami i strakhovaniya v obespechenii ustoichivosti obshchestva i ekonomiki: Sbornik trudov XXIV Mezhdunarodnoi nauchno-prakticheskoi konferentsii, 01 June 2023, Moscow, Russia.* Moscow: Lomonosov Moscow State University – Publishing House; 2023. pp. 190–194. (In Russ.).

3. Duo W., Zhou M., Abusorrah A. A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. *IEEE/CAA Journal of Automatica Sinica.* 2022;9(5):784–800. https://doi.org/10.1109/JAS.2022.105548
4. Ahmetoglu H., Das R. A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions. *Internet of Things.* 2022;20. https://doi.org/10.1016/j.iot.2022.100615
5. Shandler R., Gomez M.A. The hidden threat of cyber-attacks – undermining public confidence in government. *Journal of Information Technology & Politics*. 2023;20(4):359–374. https://doi.org/10.1080/19331681.2022.2112796
6. Saheed Y.K., Arowolo M.O. Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and Machine Learning Algorithms. *IEEE Access.* 2021;9:161546–161554. https://doi.org/10.1109/ACCESS.2021.3128837
7. Корчагин С.А., Сердечный Д.В., Раздьяконов Е.С., Беспалова Н.В. Разработка концепции обеспечения безопасности критической инфраструктуры финансового сектора. *Инженерный вестник Дона.* 2024;(4):177–186.
Korchagin S.A., Serdechnyi D.V., Razdyakonov E.S., Bespalova N.V. Development of the concept of securing the critical infrastructure of the financial sector. *Engineering Journal of Don.* 2024;(4):177–186. (In Russ.).
8. Валова Ю.И., Жмуркин И.М. Информационное обеспечение органов государственной власти РФ. *Экономика. Информатика.* 2022;49(2):243–255. https://doi.org/10.52575/2687-0932-2022-49-2-243-255
Valova Ju.I., Zhmurkin I.M. Information Support of State Authorities of the Russian Federation. *Economics. Information Technologies.* 2022;49(2):243–255. (In Russ.). https://doi.org/10.52575/2687-0932-2022-49-2-243-255
9. Преображенский Ю.П., Чопоров О.Н., Ружицкий Е. Особенности информационного обеспечения службы качества компании. *Вестник Воронежского института высоких технологий.* 2021;15(3):67–71.
Preobrazhenskiy Yu.P., Choporov O.N., Ruzhicky E. The features of information supply company quality services. *Bulletin of the Voronezh Institute of High Technologies*. 2021;15(3):67–71. (In Russ.).
10. Patterson C.M., Nurse J.R.C., Franqueira V.N.L. Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security*. 2023;132. https://doi.org/10.1016/j.cose.2023.103309
11. AI-Enhanced Cybersecurity Events Dataset. Kaggle. URL: https://www.kaggle.com/datasets/hassaneskikri/ai-enhanced-cybersecurity-events-dataset [Accessed 5th September 2024].

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Корчагин Сергей Алексеевич, кандидат физико-математических наук, доцент, ведущий научный сотрудник Института цифровых технологий, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация.
e-mail: sakorchagin@fa.ru
ORCID: 0000-0001-8042-4089

Sergey A. Korchagin, Candidate of Physical and Mathematical Sciences, Leading Researcher Institute of Digital Technologies, Financial University under the Government of the Russian Federation, Moscow, the Russian Federation.

Рубцов Дмитрий Юрьевич, аспирант кафедры информационных систем,

Dmitry Yu. Rubtsov, graduate student of the Department of Information Systems, Financial

Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация.
e-mail: dyrubtsov@fa.ru

University under the Government of the Russian Federation, Moscow, the Russian Federation.

Беспалова Наталья Викторовна, кандидат физико-математических наук, ведущий научный сотрудник Института цифровых технологий, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация.
e-mail: nvbespalova@fa.ru

Natalya V. Bespalova, candidate of physical and mathematical sciences, leading researcher at the Institute of Digital Technology, Financial University under the Government of the Russian Federation, Moscow, the Russian Federation.

Сердечный Денис Владимирович, кандидат технических наук, доцент, ведущий научный сотрудник Института цифровых технологий, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация.
e-mail: dvserdechny@fa.ru
ORCID: 0000-0003-3060-9469

Denis V. Serdechnyy, Candidate of Technical Sciences, Associate Professor, Leading Researcher at the Institute of Digital Technology, Financial University under the Government of the Russian Federation, Moscow, the Russian Federation.

Статья поступила в редакцию 20.09.2024; одобрена после рецензирования 07.10.2024; принята к публикации 14.10.2024.
The article was submitted 20.09.2024; approved after reviewing 07.10.2024; accepted for publication 14.10.2024.