# ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ ЗАЩИТЕ ИНФОРМАЦИИ

*Мещеряков Р. В.[1], Мельников С. Ю.[2], Пересыпкин В. А.[3], Хорев А. А.[4]*

**DOI:** 10.21681/2311-3456-2024-4-02-12

***Цель работы:*** *выявление актуальных направлений реализации угроз информационной безопасности различных систем с использованием технологий искусственного интеллекта и основных задач по защите информации, в которых применяются технологии искусственного интеллекта.*

***Метод исследования:*** *системный анализ открытых источников о состоянии развития современных технологий искусственного интеллекта, которые создают новые угрозы безопасности информации, и возможности применения технологий искусственного интеллекта для повышения эффективности системы защиты информации.*

***Полученный результат:*** *приведены результаты анализа основных задач защиты информации в различных направлениях информационной безопасности, в том числе использование искусственного интеллекта в компьютерных системах и сетях: обнаружение компьютерных атак; обнаружение вредоносных программ; обнаружение модификации и подмены данных и сообщений; обнаружение и предотвращение утечек конфиденциальных данных в корпоративных сетях; оценка рисков информационной безопасности; повышение надежности и киберустойчивости компьютерных систем и сетей, в вычислительных и технических системах.*

***Научная новизна:*** *систематизированы методы защиты информации с точки зрения применения технологий и систем искусственного интеллекта применительно к задаче защиты информации. Классифицированы угрозы, реализуемые с использованием технологий искусственного интеллекта: «подделка» биометрических идентификационных признаков с целью получения доступа на объект или в систему путем формирования идентификационных признаков, принадлежащих доверенному субъекту; формирование ложных речевых сообщений, имитирующих речь конкретного человека; создание ложных фото и видео с участием конкретных лиц; «подделка» текстов, имитирующих стиль определенных авторов и других.*

***Вклад авторов:*** *Мещеряков Р. В. исследовал направление по телекоммуникационным системам, Мельников С. Ю. исследовал направление по текстовым и речевым системам, Пересыпкин В. А. исследовал направление по системам аутентификации и рискориентированному подходу, Хорев А. А. исследовал направление по технической защите информации.*

***Ключевые слова:*** *информационная безопасность, защита информации, технологии искусственного интеллекта, угрозы безопасности информации, кибербезопасность.*

# PROMISING DIRECTIONS FOR APPLYING ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN INFORMATION PROTECTION

*Meshcheryakov R. V.[5], Melnikov S. Yu.[6], Peresypkin V. A.[7], Horev A. A.[8]*

1 Мещеряков Роман Валерьевич, доктор технических наук, профессор, главный научный сотрудник ИПУ РАН, Москва, Россия. ORCID: 0000-0002-1129-8434. E-mail: mrv@ieee.org

2 Мельников Сергей Юрьевич, доктор физико-математических наук, кафедра теории вероятностей и кибербезопасности института компьютерных наук и телекоммуникаций факультета физико-математических и естественных наук Российского университета дружбы народов имени Патриса Лумумбы, Москва, Россия. ORCID :0000-0002-9023-9896. E-mail: melnikov-syu@rudn.ru

3 Пересыпкин Владимир Анатольевич, доктор технических наук, действительный член Академии криптографии Российской Федерации, научный сотрудник Академии криптографии Российской Федерации, Москва, Россия. E-mail: info@cryptoacademy.gov.ru

4 Хорев Анатолий Анатольевич, доктор технических наук, профессор заведующий кафедрой информационной безопасности, МИЭТ, Москва, Россия. ORCID: 0000-0001-9074-385X. E-mail: horev@miee.ru

5 Roman V. Meshcheryakov, Dr.Sc. (of Tech.), Professor, Chief Researcher, ICS RAS, Moscow, Russia. ORCID: 0000-0002-1129-8434. E-mail: mrv@ieee.org

6 Sergey I. Melnikov, Dr.Sc. (in Physics and Math.), Department of Probability Theory and Cybersecurity, Institute of Computer Science and Telecommunications, Faculty of Physics, Mathematics and Natural Sciences, Patrice Lumumba Peoples' Friendship University of Russia, Moscow, Russia. ORCID :0000-0002-9023-9896. E-mail: melnikov-syu@rudn.ru

7 Vladimir A. Peresypkin, Dr. Sc. (of Tech.), Academician of the Academy of Cryptography of the Russian Federation, Researche, ACoRF Moscow, Russia. E-mail: info@cryptoacademy.gov.ru

8 Khorev Anatoly Anatolyevich, Dr.Sc.( of Tech.), Professor, Head of the Department of Information Security, MIET, Moscow, Russia. ORCID: 0000-0001-9074-385X. E mail: horev@miee.ru

***Purpose of the work:*** *identifying current areas of threats implementation to information security of various systems using artificial intelligence technologies and the main tasks of information protection, in which artificial intelligence technologies are used.*

***Research method:*** *system analysis of open sources and publication on the state of development of modern artificial intelligence technologies that create new threats to information security and privacy, and the possibility of using artificial intelligence technologies to improve the efficiency of the information security system.*

***Result:*** *the results of the analysis of the main tasks of information protection in various areas of information security are presented, including the use of artificial intelligence in computer systems and networks: detection of computer attacks; detection of malware; detection of modification and substitution of data and messages; detection and prevention of leaks of confidential data in corporate networks; assessment of information security risks; increasing the reliability and cyber stability of computer systems and networks, in computing and technical systems.*

***Scientific novelty:*** *the methods of information protection are systematized from the point of view of the application of artificial intelligence technologies and systems in relation to the task of information protection. The threats implemented using artificial intelligence technologies are classified: «forgery» of biometric identification features in order to gain access to an object or system by forming identification features belonging to a trusted subject; formation of false speech messages imitating the speech of a specific person; creation of false photos and videos involving specific persons; «forgery» of texts imitating the style of certain authors and others.*

***Keywords:*** *information security, information protection, artificial intelligence technologies, threats to information security, cybersecurity.*

## Введение

Развитие современных информационных технологий, с одной стороны, создает новые угрозы безопасности информации, а с другой – позволяет повысить эффективность мер защиты информации [1–3]. Технологии искусственного интеллекта являются одной из наиболее динамично развивающихся современных технологий обработки информации.

В соответствии с Национальной стратегией развития искусственного интеллекта[9] под искусственным интеллектом (ИИ) понимается комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их. Технологии искусственного интеллекта (ТИИ) включают в себя компьютерное зрение, обработку естественного языка, распознавание и синтез речи, интеллектуальную поддержку принятия решений и др.

Отметим важные изменения, внесенные в Национальную стратегию развития ИИ в 2024 году[10]. Стратегия определяет доверенные технологии ИИ как технологии, отвечающие стандартам безопасности <...>, исключающие при их использовании возможность нанесения ущерба интересам общества и государства. Обязательное внедрение доверенных технологий ИИ в тех областях его использования, в которых может быть нанесен ущерб безопасности Российской Федерации, отнесено к основным задачам развития ИИ в нашей стране. Безопасность является одним из основных принципов развития и использования ТИИ. Отмечается недопустимость использования ИИ в целях умышленного причинения вреда гражданам и организациям. Отдельно к принципам развития и использования ИИ отнесено использование ИИ в целях обеспечения информационной безопасности.

Одно из наиболее распространенных направлений использования искусственного интеллекта – это машинное обучение, которое основано на получении знаний интеллектуальной системой в процессе ее работы. Перечислим основные, широко используемые алгоритмы машинного обучения: логистическая регрессия, линейная регрессия, решающие деревья, случайный лес, градиентный бустинг, методы ближайших соседей, k-средних, опорных векторов, разновидности байесовских классификаторов, искусственные нейронные сети.

К характеристикам оценки решений с использованием технологий искусственного интеллекта относят не только ошибки первого (False Rejection Rate, «ложная тревога») и второго (False Acceptance Rate, «пропуск цели») рода. Следует использовать и обобщенные оценки, например, как в работе [4], для оценки эффективности коррекции искаженных слов в распознанных речевых сигналах используется точность и полнота (F1 мера). F1 мера – гармоническое среднее точности A и полноты R коррекций искажённого текста с одинаковым весом.

Основные задачи, которые могут решаться с использованием алгоритмов искусственного

9 Национальная стратегия развития искусственного интеллекта на период до 2030 года, утверждена Указом Президента Российской Федерации от 10 октября 2019 г. № 490.

10 Указ Президента Российской Федерации от 15.02.2024 № 124 «О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации" и в Национальную стратегию, утвержденную этим Указом».

интеллекта: классификация, кластеризация, регрессия, обнаружение аномалий, распознавание образов, поиск ассоциативных правил, прогнозирование, моделирование рассуждений, обработка естественного языка, инженерия знаний, создание экспертных систем и пр.

Множество алгоритмов искусственного интеллекта применяется как для реализации атак, так и для обеспечения защиты. Вместе с тем необходимо учитывать, что системы искусственного интеллекта могут содержать уязвимости и быть подвержены атакам различного класса, в том числе и специализированным. Одним из наиболее известных подходов к построению ландшафта угроз и поверхности атаки является база знаний MITRE ATT&CK[11].

Целью данной работы является выявление актуальных направлений реализации угроз информационной безопасности различных систем с использованием технологий искусственного интеллекта и основных задач по защите информации, в которых применяются технологии искусственного интеллекта. Указанная цель разбивается на две составные части: первая – обеспечение защиты от атак, которые реализуются с использованием технологий искусственного интеллекта, вторая – использование технологий искусственного интеллекта для защиты от угроз информационной безопасности.

### 1.Анализ возможных угроз безопасности информации, создаваемых с использованием технологий искусственного интеллекта

Исторически первые методы ИИ применялись в задачах идентификации, связанных с обработкой речи, текста и изображений. В настоящее время идентификация по биометрическим признакам уже широко используется в системах управления доступа на объектах информатизации, в автоматизированных и информационных системах различного назначения. Сегодня биометрические системы используются в большинстве смартфонов.

Особенностью использования ТИИ является возможность сбора и обработки огромного объема биометрических идентификационных признаков, таких как: изображения лица, формы кисти, отпечатков пальцев, особенностей голоса, клавиатурного почерка или почерка на графическом планшете и т.д. [5–10].

К возможным угрозам, реализуемым с использованием ТИИ по обработке биометрических идентификационных признаков, можно отнести следующие:

- «подделка» биометрических идентификационных признаков с целью получения прав доступа на объект или в систему путем формирования идентификационных признаков другого лица, как, например, это сделано с отпечатками пальцев[12] или речевыми сообщениями [11–13];
- формирование ложных речевых сообщений, имитирующих речь конкретного человека [8];
- создание ложных фото и видео с участием конкретных лиц [11];
- «подделка» текстов, имитирующих стиль определенных авторов [9] и т.д.

Указанные угрозы биометрических систем с использованием подходов на базе ИИ потенциально нарушают не только конфиденциальность и доступность информации, но и ее целостность, т.к. в ходе реализации угрозы может производиться подмена информации. Известны случаи подделки не только внешних, наглядно различимых идентификационных признаков, но и тех признаков, которые являются «внутренними» и связаны с личностными, социальными и иными поведенческими реакциями. Это существенно усложняет противодействие такого рода атакам.

Следовательно, возникают задачи противодействия новым угрозам безопасности информации, которые возникают в результате использования технологий искусственного интеллекта. В частности, следует отметить:

- выявление, локализация источника угроз, который использует технологии искусственного интеллекта;
- классификация вида угроз для конкретного объекта и технологии защиты, против которого направлена угроза и формируется новое признаковое пространство угрозы (включая вектор атаки);
- моделирование действий конкретного типа злоумышленника, под действия которого моделируется проведение атаки, реализующая конкретную угрозу и происходит мимикрия под конкретный источник угроз;
- переход от статического к динамическому обнаружению угроз (например, как используется биометрическая технология liveness), однако и это направление в настоящее время отрабатывается злоумышленниками на высоком уровне;
- информационное противоборство с учетом ретроспективных и прогнозных моделей для формирования целевой линии поведения системы защиты для выявления аномалий, генерируемых системами с искусственным интеллектом, обученными на моделях подыгрывающей стороны;
- возможности реализации новых угроз с использованием генеративных моделей ИИ при формировании открытого признакового пространства

11 MITRE ATT&CK https://attack.mitre.org/

12 Универсальные отпечатки» для взлома смартфонов https://sysblok.ru/futurology/universalnye-otpechatki-dlja-vzloma-smartfonov/

сигнальных последовательностей на входе в информационную систему и систему защиты информации;
- угроза генерации «отложенного» внутреннего нарушителя, который запускается при возникновении определенных событий.

Таким образом, отмеченные задачи требуют проработки не только на уровне построения моделей нарушителей и моделей угроз, но и с учетом динамики развития потенциально возможных злоумышленных действий, которые необходимо учитывать при формировании обучающих выборок сценариев деятельности системы защиты информации.

### 2. Анализ возможных направлений использования технологий искусственного интеллекта при решении задач защиты информации

Наиболее распространенной областью применения технологий искусственного интеллекта в целях защиты информации являются автоматизированные, информационные, киберфизические и телекоммуникационные системы, включая компьютерные сети различной архитектуры (далее компьютерные системы и сети).

К основным задачам защиты информации в компьютерных системах и сетях с использованием искусственного интеллекта можно отнести:

- обнаружение компьютерных атак;
- обнаружение вредоносных программ;
- обнаружение модификации и подмены данных и сообщений;
- обнаружение и предотвращение утечек конфиденциальных данных в корпоративных сетях;
- оценка рисков информационной безопасности;
- повышение надежности и киберустойчивости компьютерных систем и сетей.

Недостатки традиционных систем информационной безопасности во многом связаны с тем, что они основаны на правилах. Используются заранее определенные методы выявления угроз и реагирования на них. Это влечет за собой ограничения, в частности неспособность реагировать на новые угрозы. С появлением новых угроз правила обновляют вручную. Другим таким ограничением является объем данных. Существующие системы безопасности могут генерировать огромные объемы данных, которые сложно анализировать в реальном времени. Кроме того, системы, основанные на правилах, могут оказаться неэффективными при обнаружении более сложных атак, например использующих ИИ для имитации обычного поведения пользователя.

#### Преимущества технологий искусственного интеллекта

Возможность быстрой обработки больших массивов данных для «раннего предупреждения». Это одно из ключевых преимуществ ИИ. С помощью ИИ можно в режиме реального времени анализировать огромные объемы информации, прежде всего сетевого трафика.

Обнаружение аномалий и необычной активности. ИИ может анализировать данные из нескольких источников, включая сетевой трафик, системные журналы и данные о поведении пользователей, чтобы выявлять активности, выходящие за рамки нормы. Например, ИИ может обнаружить необычные модели поведения, которые могут указывать на кибератаку, например, передачу больших объемов данных во внешнюю систему или необычные попытки входа в систему. ИИ может провести анализ поведения пользователей, чтобы выявлять аномалии, которые могут указывать на внутреннюю угрозу, например, когда сотрудник получает доступ к данным в нерабочее время или получает доступ к данным, на доступ к которым у него обычно нет разрешения.

Автоматизация реагирования на угрозы. Еще одним преимуществом ИИ в информационной безопасности является его способность автоматизировать реагирование на угрозы. Например, если система искусственного интеллекта обнаруживает попытку кибератаки, она может автоматически заблокировать доступ к скомпрометированной системе, предотвращая дальнейший ущерб. Он также может отправлять оповещения сотрудникам службы безопасности, предоставляя им информацию об инциденте.

Новым, пока еще не сильно развитым направлением является использование методов ИИ для анализа систем шифрования и оценки качества генераторов псевдослучайных чисел (ГПСЧ). Существующие подходы с использованием нейросетей для анализа блочных шифров очень ограничены и представляют научный интерес для слабых шифров, у которых минимизированы число раундов и ослаблены другие важные криптографические параметры. Больший интерес представляет атака на ГСПЧ, которая может определять отклонения от случайности и прогнозировать следующие элементы выходной последовательности ГПСЧ, если известны несколько предшествующих. Так, подход с использованием глубоких нейросетей предложен в [15] для анализа модифицированного линейного конгруэнтного генератора.

Отметим, что в последние годы появляются работы, в которых методы ИИ применяются и для анализа квантовых генераторов случайных чисел ([16, 17] и др.).

При обнаружении компьютерных атак и вредоносных программ отметим направление UEBA (User and Entity Behavior Analytics) – системы поведенческого анализа пользователей и информационных сущностей. Основной сценарий применения ИИ-технологий в продуктах типа UEBA – это выявление аномалий в поведенческих моделях пользователей информационных систем. Выявленные аномалии могут классифицироваться с помощью тех или иных методов ИИ.

### Оценка риска с использованием технологий искусственного интеллекта

Следует отразить особенность – это вероятностное описание объекта защиты, применительно к которому проводится оценка риска. Существующий арсенал моделей и подходов к оценке рисков позволяет использовать как вербальные описания, так и формализованные по стандартам менеджмента качества [18–30]. Очевидно, что расчет рисков очень важен для объектов критической информационной инфраструктуры (например, предприятий ТЭК), и беспилотных транспортных средств [31, 32].

С учетом большого количества данных, которые могут быть использованы для обучения, и наличия специализированных вычислителей распространенным решением является использование искусственных нейронных сетей [33–40]. Применению их в системах информационной безопасности посвящен ряд работ [41–44]. Для разных задач, разных обучающих выборок, разных конфигураций доступных вычислителей необходим творческий этап выбора подходящей нейросетевой архитектуры. В качестве обучающей выборки наиболее распространен датасет NSL-KDD Dataset[13].

Задачи информационной безопасности, характерные для новых типов сетей (киберфизические системы, сети интернета вещей и др.) [45–51], имеют свои особенности. Отметим расширяющееся использование биоинспирированных подходов для обеспечения безопасности сетей. В частности, идея иммунных подходов к безопасности сетей состоит в постоянном внутреннем мониторинге работы сети, идентификации зараженного сетевого узла и блокировке этого узла. Указанный подход использовался на заре развития интернета, но в то время не было надежных средств оценки рисков, что часто приводило к некорректным отключениям пользователей.

### Анализ возможных направлений решения задач защиты информации для обеспечения безопасности технологий искусственного интеллекта

Отдельным направлением обеспечения информационной безопасности является обеспечение безопасности самих систем искусственного интеллекта, включая системы машинного обучения.

13 NSL-KDD Dataset https://www.unb.ca/cic/datasets/nsl.html

Национальной стратегией развития искусственного интеллекта к числу новых вызовов для государства отнесено, в том числе, «возникновение в сфере разработки, создания и использования ТИИ новых типов угроз информационной безопасности, нехарактерных для других сфер применения информационных технологий». Речь идет, в том числе, о специфических угрозах: атаки на обучающие данные, искажение разметки, атаки, направленные на установление принадлежности конкретных данных обучающей выборке, атаки, направленные на получение данных из обученной модели, и др.

Следовательно, для защиты систем искусственного интеллекта наряду с типовыми средствами защиты информации должны использоваться и специфические технологии, и средства защиты, к основным из которых можно отнести: повышение надежности обучающих выборок, оценка доверия к принимаемым решениям, интерпретируемость результатов, контроль процессов обучения и верификации, повторяемость, отсутствие галлюцинаций и другие.

Наиболее распространенные способы защиты от вредоносных воздействий на обучающие данные, обнаружения выбросов (аномалий) и проверки точности модели машинного обучения приведены в работах [53–60].

Известно, что архитектуры и принципы работы различных систем искусственного интеллекта существенно отличаются друг от друга, но для оценивания возможности атак на системы искусственного интеллекта надо учитывать следующие характеристики: точность (следует отличать работу на тестовых выборках и в реальных условиях), интерпретируемость (одна из наиболее важных характеристик, которая показывает, что система в состоянии объяснить принятое решение), параметрические или непараметрические модели (имеется ли заранее известные гипотезы и предположения), размерность данных для обработки, требуемая вычислительная архитектура (процессоры общего назначения, графические и нейроморфные).

Перечислим основные векторы атак на системы искусственного интеллекта, которые отражены в отчете по уязвимостям SonicWall[14]:

- искажение разметки;
- искажение обучающей выборки;
- атаки «белого ящика» и «черного ящика»;
- атаки на предобученные и аутсорсинговые ML-модели;
- утечки через обученные модели, атаки на уровне аппаратного обеспечения.

При рассмотрении различных систем следует

14 2022 SonicWall Cyber Threat Report https://www.infopoint-security.de/media/2022-sonicwall-cyber-threat-report.pdf

отметить, что возможны атаки на криптографические алгоритмы с использованием технологий ИИ, а также на стеганографические алгоритмы для проведения стегоанализа [61].

В акустическом и радио каналах утечки информации следует уделять большое значение проведению моделирования свойств канала, поведению злоумышленника, работе средств перехвата и средств защиты. Технологии искусственного интеллекта используются как для «проигрывания» различных сценариев, так и для обработки сигналов, которые регистрируются в канале утечки. Очевидно, что с использованием искусственного интеллекта появляется возможность проведения анализа сигналов с учетом фоновой обстановки и последующей его интерпретации, поиска полезных сигналов [62–77].

Развитие средств физический защиты и нападения в настоящее время использует повышение интеллектуализации (читай искусственного интеллекта) для обеспечения периметровой охраны. Средства интеллектуализации позволяют провести моделирование различных угроз и поведения нарушителя, а также обеспечить на рубежах охраны контроль с использование средств распознавания. Следует учитывать, что даже использование воздушного зазора в критических системах не позволяет быть уверенными в безопасности всей системы.

Следует отметить, что алгоритмы искусственного интеллекта могут быть использованы и для исследования организационно-социальных и политических направлений [78]. Использование систем искусственного интеллекта с языковыми моделями типа ChatGPT для получения различной аналитической информации позволяет повысить эффективности деятельности аналитических подразделений. Спектр применения больших языковых моделей очень широк и позволяет не только проводить указанную аналитическую деятельность и конкурентную разведку, но и генерировать уникальный контент, в том числе вредоносный и ложный «человекоподобный», который используется для проведения атак социальной инженерии, например, фишинга с использованием телефонного канала.

Ряд систем генеративного искусственного интеллекта подвержены не только «переобучениям». Результатом запроса информации в таких системах может быть информация, которая отсутствует в обучающей выборке, может противоречить ей, однако по структуре соответствует реальной информации – этот результат называют «галлюцинацией». Указанная уязвимость может быть эксплуатируема злоумышленниками, а противодействие ей может быть осуществлено только путем создания доверенного искусственного интеллекта [79] за счет объяснимости и верификации выходных результатов работы.

## Заключение

Актуальность использования технологий искусственного интеллекта в области обеспечения безопасности приобретает решающее значение. Тот, кто будет владеть технологиями, тот и будет превосходить противника вне зависимости от выполняемой атакующей или нападающий функции. Представляется важным нормативно регулировать деятельность систем искусственного интеллекта [80].

Рассмотренные в настоящей статье подходы систематизируют использование ИИ для обеспечения безопасности и защиты информации от утечек по различным техническим каналам, а также целостности и доступности. Развитие технологий искусственного интеллекта для обработки сигналов и данных различной природы будет ставить перед специалистами по защите информации новые задачи, формировать требования к средствам защиты и к разработке моделей каналов утечки информации.

*Работа выполнена при финансовой поддержке гранта РНФ № 24-11-00340*

**Литература**

1. *Марков А. С. Кибербезопасность и информационная безопасность как бифуркация номенклатуры научных специальностей // Вопросы кибербезопасности. 2022, № 1(47), с. 2–10.*
2. *Язов Ю. К. О научных специальностях «кибербезопасность» и «Методы и системы защиты информации. Информационная безопасность» // Вопросы кибербезопасности. 2022, № 2(48), с. 5-6.*
3. *Толстой А. И. Систематика понятий в области информационной безопасности. Безопасность информационных технологий, 2023, т. 30, № 1, с. 130–148.*
4. *Мельников С. Ю., Пересыпкин В. А. Об эволюции классических вероятностных моделей языка в естественно-языковых приложениях. Вестник современных цифровых технологий. 2023, № 16, с. 4–14.*
5. *Информационные измерения языка. Программная система оценки читаемости искаженных текстов / А. В. Германович, С. Ю. Мельников, В. А. Пересыпкин [и др.] // Известия ЮФУ. Технические науки. 2019, № 7 (209), с. 6–17.*
6. *Иванов А. И., Сулавко А. Е. Проект третьего национального стандарта России по быстрому автоматическому обучению больших сетей корреляционных нейронов на малых обучающих выборках биометрических данных // Вопросы кибербезопасности. 2021, № 3(43), с. 84–93.*

7. Машкина И. В., Белова Е. П. Разработка нейросетевой базы данных биометрических образов на основе нескольких параметров спектров гласных звуков для системы аутентификации и авторизации по голосу // Безопасность информационных технологий. 2019, т. 26, № 3, с. 90–102.
8. Костюченко Е. Ю., Мещеряков Р. В. Идентификация по биометрическим параметрам при использовании аппарата нейронных сетей // Нейрокомпьютеры: разработка, применение. 2007, № 7, с. 39–50.
9. Матвеев Ю. Н. Технологии биометрической идентификации личности по голосу и другим модальностям // Вестник Московского государственного технического университета им. Н.Э. Баумана. 2012, № 3 (3), с. 5–15.
10. Ziems N., Wu S. Security Vulnerability Detection Using Deep Learning Natural Language Processing, IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops, 2021, pp. 1–6.
11. Morris J. X. et al. Textattack: A framework for adversarial attacks in natural language processing. 2020. DOI: https://doi.org/10.48550/arXiv.2005.05909.
12. Сидняев Н. И., Синева Е. Е. Построение составных критериев для оптимизации термов и обобщенного показателя баз знаний интеллектуальных систем // Вопросы кибербезопасности. 2023, № 2(54), с. 23–35.
13. Васильев В. И., Вульфин А. М., Кучкарова Н. В. Тематическое моделирование и суммаризация текстов в области кибербезопасности // Вопросы кибербезопасности. 2023, № 2(54), с. 2–22.
14. Baek S., Kim K. Recent advances of neural attacks against block ciphers //Proc. of SCIS. 2020.
15. Amigo G., Dong L., Ii R. J. M. Forecasting pseudo random numbers using deep learning // 2021 15th International Conference on Signal Processing and Communication Systems (ICSPCS). – IEEE, 2021. pp. 1–7.
16. Feng Y., Hao L. Testing randomness using artificial neural network //IEEE Access. 2020, Vol. 8, pp. 163685-163693.
17. Truong N. D. et al. Machine learning cryptanalysis of a quantum random number generator //IEEE Transactions on Information Forensics and Security. 2018, Т. 14, №. 2, с. 403–414.
18. Язов Ю. К., Соловьев С. В., Тарелкин М. А Логико-лингвистическое моделирование угроз безопасности информации в информационных системах // Вопросы кибербезопасности. 2022, № 4(50), с. 13–25.
19. Васильев В. И., Вульфин А. М., Герасимова И. Б., Картак В. М. Анализ рисков кибербезопасности с помощью нечетких когнитивных карт // Вопросы кибербезопасности. 2020, № 2(36), с. 11–21.
20. Васильев В. И., Вульфин А. М., Кучкарова Н. В. Оценка актуальных угроз безопасности информации с помощью технологии трансформеров // Вопросы кибербезопасности. 2022, № 2(48), с. 27–38.
21. Плугатарев А. В. и др. Применение нейронных сетей в системах обеспечения информационной безопасности // Безопасность информационных технологий, 2021, т. 28, № 3, с. 73–80.
22. Парьев С. Е., Правиков Д. И., Карантаев В. Г. Особенности применения риск-ориентированного подхода для обеспечения кибербезопасности промышленных объектов // Безопасность информационных технологий. 2020, т. 27, № 4, с. 37–52.
23. Воеводин В. А. Модель оценки функциональной устойчивости элементов информационной инфраструктуры для условий воздействия множества компьютерных атак. Информатика и автоматизация, 2023, 22(3), с. 691–715
24. Селифанов В. В., Солдатов А. Ю., Солдатов Е. Ю., Подлегаев А. П., Скориков В. С. Метод оценивания рисков в системах принятия решений с учетом защиты информации. Вестник СибГУТИ. 2023; 17(2). с. 84–92.
25. Ермаков С. А., Чурсин А. Г., Болгов А. А. Нечетко-множественная методика оценки рисков автоматизированной системы «Умный дом» с динамической топологией Информация и безопасность. 2022, Том: 25, № 4, с. 495–500.
26. Ермаков С. А., Болгов А. А. Оценка риска с использованием нейро-нечеткой системы // Информация и безопасность. 2022, Том: 25, № 4, с. 583–592.
27. Ермаков С. А., Гусарева Ю. А., Болгов А. А., Кострова В. Н. Повышение защищенности автоматизированной системы «умный дом»: алгоритм оценки рисков нарушения конфиденциальности информации // Информация и безопасность. 2022, Том: 25, № 3, с. 377–388.
28. Космачева И. М., Давидюк Н. В., Сибикина И. В., Кучин И. Ю. Модель оценки эффективности конфигурации системы защиты информации на базе генетических алгоритмов // Моделирование, оптимизация и информационные технологии. 2020; 8(3). Доступно по: https://moit.vivt.ru/wp-content/uploads/2020/08/KosmachevaSoavtors_3_20_1.pdf DOI: 10.26102/2310-6018/2020.30.3.022.
29. Семенов В. В. Оценивание состояния информационной безопасности на основе анализа временных рядов // Научно-технический вестник Поволжья. 2021, № 10, с. 127–129.
30. Рычкова А. А., Бурькова Е. В., Коннов А. Л. Анализ угроз информационной безопасности на основе метода кластеризации данных // Научно-технический вестник Поволжья. 2023, № 6, с. 307–310.
31. Промыслов В. Г., Акимов Н. Н., Абдулова Е. А., Голубев П. А., Жарко Е. Ф., Жмайлов В. В., Лепехин И. Ю., Лобанок О. И., Исхаков А. Ю., Мещеряков Р. В., Полетыкин А. Г., Мусихин А. М., Пронин В. В., Семенков К. В., Цыренов Д. В. Оценка риска и обеспечение кибербезопасности атомных электростанций. М.: ИПУ РАН, 2022. – 193 с.
32. Жарко Е. Ф., Промыслов В. Г., Исхаков А. Ю., Мещеряков Р. В., Семенков К. В., Абдулова Е. А., Байбулатов А. А., Исхаков С. Ю. Кибербезопасность беспилотных транспортных средств. Архитектура. Методы проектирования. М.: Радиотехника, 2021. – 160 с.
33. Ветров И. А., Подтопельный В.В. Особенности формирования вектора современных сетевых атак. Вестник СибГУТИ. 2022, № 3, с. 3–13.
34. Мещеряков Р. В., Исхаков А. Ю., Евсютин О. О. Современные методы обеспечения целостности данных в протоколах управления киберфизических систем. Информатика и автоматизация. 2020, 19(5), с. 1089–1122.
35. Букин А. В., Самонов А. В., Тихонов Э. И. Обнаружение инцидентов информационной безопасности на основе технологии нейронных сетей // Вопросы кибербезопасности. 2022, № 5(51), с. 61–73.
36. Саенко И. Б., Котенко И. В., Аль-Барри М. Х. Применение искусственных нейронных сетей для выявления аномального поведения пользователей центров обработки данных // Вопросы кибербезопасности. 2022, № 2(48), с. 87–97.
37. Меркальдо Ф., Мартинелли Ф., Сантоне А. Проверка модели для обнаружения атак в реальном времени в системах распределения воды. Информатика и автоматизация. 2022, 21(2), с. 219–242.
38. Штыркина А. А. Метод реконфигурации топологии киберфизической системы на основе графовой искусственной нейронной сети // Проблемы информационной безопасности. Компьютерные системы. 2023, 2 (54), с. 173–182.

39. *Сергадеева А. И., Лаврова Д. С. Применение модульной нейронной сети для обнаружения DDOS-атак // Проблемы информационной безопасности. Компьютерные системы 2023, № 1 (53), с. 111–118.*
40. *Александрова Е. Б., Штыркина А. А. Метод адаптивной нейтрализации структурных нарушений киберфизических систем на основе графовых искусственных нейронных сетей // Проблемы информационной безопасности. Компьютерные системы. 2023, № 4 (52), с. 89-100.*
41. *Царькова Е. Г. К вопросу применения искусственных нейронных сетей в системах обеспечения транспортной безопасности // Проблемы информационной безопасности. Компьютерные системы. 2022, Том: 3, № 3 (3), с. 28–34.*
42. *Кубасов И. А., Сушков В. И. Применение технологий искусственного интеллекта в робототехнических комплексах специального назначения в целях обеспечения правоохранительной деятельности // Вестник Воронежского института ФСИН России. 2022, № 3, с. 69–76.*
43. *Алексеенко С. П., Достов В. В. Нейросети и информационная безопасность в правоохранительных структурах // Охрана, безопасность, связь. 2022, № 7-2, с. 11–16.*
44. *Атаки на искусственный интеллект. Как защитить машинное обучение в системах безопасности. Александр Чистяков, Алексей Андреев «Лаборатория Касперского», Департамент исследования угроз. https://media.kaspersky.com/ru/business-security/attacks-on-artificial-intelligence-whitepaper.pdf*
45. *Котенко И. В., Саенко И. Б., Лаута О. С., Крибель А. М. Методика обнаружения аномалий и кибератак на основе интеграции методов фрактального анализа и машинного обучения. Информатика и автоматизация, 2022, 21(6), с. 1328–1358.*
46. *Зегжда Д. П., Калинин М. О., Крундышев В. М., Лаврова Д. С., Москвин Д. А., Павленко, Е. Ю. Применение алгоритмов биоинформатики для обнаружения мутирующих кибератак // Информатика и автоматизация, 2021, 20(4), с. 820–844.*
47. *Калинин М. О., Ткачева Е. И. Децентрализованный подход к обнаружению вторжений в динамических сетях интернета вещей на базе многоагентного обучения с подкреплением и межагентным взаимодействием // Проблемы информационной безопасности. Компьютерные системы. 2023, № 2 (54), с. 202–211.*
48. *Калинкин А. О. и др. Обнаружение программ-шифровальщиков на основе данных механизма трассировки событий и применения метода машинного обучения // Безопасность информационных технологий. 2022, т. 29, № 3, с. 82–93.*
49. *Синюк А. Д., Остроумов О. А., Тарасов А. А. (). Теоретико-информационное представление виртуализации сетевого канала перехвата // Информатика и автоматизация. 2023, 22(4), с. 721–744.*
50. *Макарова О. С., Поршнев С. В. Оценивание вероятностей компьютерных атак на основе функций // Безопасность информационных технологий. 2020, т. 27, № 2, с. 86–96.*
51. *Марков Г. А., Крундышев В. М., Калинин М. О., Зегжда Д. П., Бусыгин А. Г. Обнаружение компьютерных атак в сетях промышленного интернета вещей на основе вычислительной модели иерархической временной памяти // Проблемы информационной безопасности. Компьютерные системы. 2023, № 2 (54), с. 163–172.*
52. *Мещеряков Р.В., Исхаков С.Ю. Исследование индикаторов компрометации для средств защиты информационных и киберфизических систем // Вопросы кибербезопасности. 2022, № 5 (51), с. 82–99.*
53. *Павлова К. С. Применение предметных онтологий в области обеспечения безопасности информации // Проблемы информационной безопасности. Компьютерные системы. 2023, Том: 1, № 1 (1), с. 24–29.*
54. *Ручай А. Н., Токарев И. В., Грибачёв А. С. Методы машинного обучения и искусственного интеллекта в сфере информационной безопасности: анализ современного состояния и перспективы развития // Вестник УрФО. Безопасность в информационной сфере. 2022, 4 (46), с. 76–87.*
55. *Артамонов В. А., Артамонова Е. В., Сафонов А. Е. Безопасность искусственного интеллекта // Защита информации. Инсайд. 2022, № 6 (108), с. 8–17.*
56. *Артамонов В. А., Артамонова Е. В. Искусственный интеллект в системах безопасности // Защита информации. Инсайд. 2022, № 5 (107), с. 40–49.*
57. *Лебедев И. С., Сухопаров М. Е. Использование информации о влияющих факторах для разбиения выборок данных в методах машинного обучения для оценки состояния ИБ // Проблемы информационной безопасности. Компьютерные системы. 2023, №2 (54), с. 125–134.*
58. *Sarker I., Kayes A., Badsha S., Alqahtani H., Watters P., Ng A. Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 2020.*
59. *Musser M., Garriott A. Machine Learning and Cybersecurity. Center for Security and Emerging Technology, 2021.*
60. *Чекмарев М. А., Клюев С. Г., Бобров Н. Д. Анализ методов обеспечения безопасности систем машинного обучения. Моделирование, оптимизация и информационные технологии. 2022; 10(1). DOI: 10.26102/2310-6018/2022.36.1.006*
61. *Evsutin O., Melman A., Meshcheryakov R. Digital steganography and watermarking for digital images: a review of current research directions IEEE Access. 2020, Vol. 8, pp. 166589–166611.*
62. *Хорев А. А. Некоторые подходы к оценке возможностей перехвата побочных электромагнитных излучений средств вычислительной техники, использующих цифровые интерфейсы // Вестник УрФО. Безопасность в информационной сфере. 2022, № 3 (45), с. 5–16.*
63. *Сычев М. П., Мазин А. В., Зеленцова Е. В., Крылов В. О., Сидельников А. П. Функциональные аспекты моделирования процесса перехвата информативных сигналов по параметрическим каналам // Приборы и системы. Управление, контроль, диагностика. 2022, № 2, с. 22–33.*
64. *Сычев М. П., Никулин С. С., Маньков Е. А. Перехват информации по параметрическим каналам: структуризация функционального представления этапа обработки перехваченных информативных сигналов с целью формирования целостного объема информации об объекте разведки // Вестник Воронежского института МВД России. 2023, № 2, с. 87–93.*
65. *Мещеряков Р. В., Лось В. П., Щербаков В. А., Рекунков И. С. Математическое моделирование защитных экранов для предотвращения утечки информации по техническим каналам в радиодиапазоне // Вопросы защиты информации. 2023, № 1 (140), с. 47–52.*
66. *Копытов П. Д., Королёв И. Д., Кулиш О. А., Степанцов С. В. Построение формальных моделей распространения побочных электромагнитных излучений по техническим каналам утечки информации для объектов вычислительной техники от технических средств разведки // Вестник УрФО. Безопасность в информационной сфере. 2023, № 1 (47), с. 102–111.*

67. Захаров А. В. Требования к современному программно-аппаратному комплексу радиоконтроля и цифрового анализа сигналов // Защита информации. Инсайд. 2022, № 1 (103), с. 24–33.
68. Алексеенко С. П., Антиликаторов А. Б., Астахов Н. В. Методика выбора модели охраны объекта радиотехническими средствами обнаружения // Вестник Воронежского института МВД России. 2023, № 1, с. 57–62.
69. Аверьянов А. А., Шадрив В. В., Бердюгин В. Ю. Математическая модель оценки угроз физического проникновения злоумышленника на защищенный объект // Вестник УрФО. Безопасность в информационной сфере. 2022, № 4 (46), с. 52–57.
70. Язов Ю. К., Соловьев С. В., Тарелкин М. А. Применение составных сетей Петри-Маркова при математическом моделировании угроз безопасности информации // Охрана, безопасность, связь. 2023, № 8–2, с. 185–196.
71. Авсентьев А. О. Проблема построения многоагентных систем защиты информации на объектах информатизации от утечки по техническим каналам // Вестник Воронежского института МВД России. 2022, № 3, с. 68–77.
72. Калач А. В., Здольник В. В. Математическая модель показателя эффективности мер, направленных на предотвращение утечки информации по каналам побочных электромагнитных излучений и наводок. Вестник Воронежского института ФСИН России. 2022, № 1, с. 54–61.
73. Минаев В. А., Коробец Б. Н., Сычев М. П., Севрюков Д. В., Дудоладов В. А. Ключевые функциональные показатели радиотехнических средств обнаружения проникновения на охраняемые объекты // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2019, № 5–6 (131-132), с. 3–7.
74. Алексеев Д. С., Козлов Р. С. Метод практической оценки эффективности средств активной защиты от утечки конфиденциальной информации по техническому каналу // Научно-технический вестник Поволжья. 2023, № 4, с. 201–204.
75. Бурькова Е. В., Рычкова А. А. Методика принятия решений при выборе средств физической защиты на основе метода анализа иерархии // Научно-технический вестник Поволжья. 2021, № 5, с. 119–123.
76. Авсентьев О. С., Вальде А. Г. Вербальная модель защиты информации от утечки по техническим каналам в процессе формирования системы защиты информации на объектах информатизации // Вестник Воронежского института МВД России. 2022, № 2, с. 18–27.
77. Пантюхов Д. В., Логинов И. В. Варианты построения интеллектуальных систем физической безопасности с учетом развития технологий интеллектуализации // Охрана, безопасность, связь. 2023, № 8-1, с. 155–159.
78. Костогрызов А. И. Подход к вероятностному прогнозированию защищенности репутации политических деятелей от «фейковых» угроз в публичном информационном пространстве // Вопросы кибербезопасности. 2023, № 3 (55), с. 114–133
79. Аветисян А. И. Использование доверенного ПО при создании систем искусственного интеллекта как основа безопасности (доклад) // XXVII научно-практическая конференция «Комплексная защита информации», 24–26 мая 2022 года, Московская область.
80. Гарбук С. В. Задачи нормативно-технического регулирования интеллектуальных систем информационной безопасности // Вопросы кибербезопасности. 2021, № 3 (43), с. 68–83.

## References

1. Markov A. S. Kiberbezopasnost' i informacionnaja bezopasnost' kak bifurkacija nomenklatury nauchnyh special'nostej // Voprosy kiberbezopasnosti. 2022, № 1(47), s. 2–10.
2. Jazov Ju. K. O nauchnyh special'nostjah «kiberbezopasnost'» i «Metody i sistemy zashhity informacii. Informacionnaja bezopasnost'» // Voprosy kiberbezopasnosti. 2022, № 2(48), s. 5-6.
3. Tolstoj A. I. Sistematika ponjatij v oblasti informacionnoj bezopasnosti. Bezopasnost' informacionnyh tehnologij, 2023, t. 30, № 1, s. 130–148.
4. Mel'nikov S. Ju., Peresypkin V. A. Ob jevoljucii klassicheskih verojatnostnyh modelej jazyka v estestvenno-jazykovyh prilozhenijah. Vestnik sovremennyh cifrovyh tehnologij. 2023, № 16, s. 4–14.
5. Informacionnye izmerenija jazyka. Programmnaja sistema ocenki chitaemosti iskazhennyh tekstov / A. V. Germanovich, S. Ju. Mel'nikov, V. A. Peresypkin [i dr.] // Izvestija JuFU. Tehnicheskie nauki. 2019, № 7 (209), s. 6–17.
6. Ivanov A. I., Sulavko A. E. Proekt tret'ego nacional'nogo standarta Rossii po bystromu avtomaticheskomu obucheniju bol'shih setej korreljacionnyh nejronov na malyh obuchajushhih vyborkah biometricheskih dannyh // Voprosy kiberbezopasnosti. 2021, № 3(43), s. 84–93.
7. Mashkina I. V., Belova E. P. Razrabotka nejrosetevoj bazy dannyh biometricheskih obrazov na osnove neskol'kih parametrov spektrov glasnyh zvukov dlja sistemy autentifikacii i avtorizacii po golosu // Bezopasnost' informacionnyh tehnologij. 2019, t. 26, № 3, s. 90–102.
8. Kostjuchenko E. Ju., Meshherjakov R. V. Identifikacija po biometricheskim parametram pri ispol'zovanii apparata nejronnyh setej // Nejrokomp'jutery: razrabotka, primenenie. 2007, № 7, s. 39–50.
9. Matveev Ju. N. Tehnologii biometricheskoj identifikacii lichnosti po golosu i drugim modal'nostjam // Vestnik Moskovskogo gosudarstvennogo tehnicheskogo universiteta im. N.Je. Baumana. 2012, № 3 (3), s. 5–15.
10. Ziems N., Wu S. Security Vulnerability Detection Using Deep Learning Natural Language Processing, IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops, 2021, pp. 1–6.
11. Morris J. X. et al. Textattack: A framework for adversarial attacks in natural language processing. 2020. DOI: https://doi.org/10.48550/arXiv.2005.05909.
12. Sidnjaev N. I., Sineva E. E. Postroenie sostavnyh kriteriev dlja optimizacii termov i obobshhennogo pokazatelja baz znanij intellektual'nyh sistem // Voprosy kiberbezopasnosti. 2023, № 2(54), s. 23–35.
13. Vasil'ev V. I., Vul'fin A.M., Kuchkarova N. V. Tematicheskoe modelirovanie i summarizacija tekstov v oblasti kiberbezopasnosti // Voprosy kiberbezopasnosti. 2023, № 2(54), s. 2–22.
14. Baek S., Kim K. Recent advances of neural attacks against block ciphers //Proc. of SCIS. 2020.
15. Amigo G., Dong L., Ii R. J. M. Forecasting pseudo random numbers using deep learning // 2021 15th International Conference on Signal Processing and Communication Systems (ICSPCS). – IEEE, 2021. pp. 1–7.
16. Feng Y., Hao L. Testing randomness using artificial neural network //IEEE Access. 2020, Vol. 8, pp. 163685–163693.
17. Truong N. D. et al. Machine learning cryptanalysis of a quantum random number generator //IEEE Transactions on Information Forensics and Security. 2018, T. 14, №. 2, s. 403–414.

18. Jazov Ju. K., Solov'ev S. V., Tarelkin M.A Logiko-lingvisticheskoe modelirovanie ugroz bezopasnosti informacii v informacionnyh sistemah // Voprosy kiberbezopasnosti. 2022, № 4(50), s. 13–25.
19. Vasil'ev V. I., Vul'fin A. M., Gerasimova I. B., Kartak V. M. Analiz riskov kiberbezopasnosti s pomoshh'ju nechetkih kognitivnyh kart // Voprosy kiberbezopasnosti. 2020, № 2(36), s. 11–21.
20. Vasil'ev V. I., Vul'fin A. M., Kuchkarova N. V. Ocenka aktual'nyh ugroz bezopasnosti informacii s pomoshh'ju tehnologii transformerov // Voprosy kiberbezopasnosti. 2022, № 2(48), s. 27–38.
21. Plugatarev A. V. i dr. Primenenie nejronnyh setej v sistemah obespechenija informacionnoj bezopasnosti // Bezopasnost' informacionnyh tehnologij, 2021, t. 28, № 3, s. 73–80.
22. Par'ev S. E., Pravikov D. I., Karantaev V. G. Osobennosti primenenija risk-orientirovannogo podhoda dlja obespechenija kiberbezopasnosti promyshlennyh ob#ektov // Bezopasnost' informacionnyh tehnologij. 2020, t. 27, № 4, s. 37–52.
23. Voevodin V. A. Model' ocenki funkcional'noj ustojchivosti jelementov informacionnoj infrastruktury dlja uslovij vozdejstvija mnozhestva komp'juternyh atak. Informatika i avtomatizacija, 2023, 22(3), s. 691–715
24. Selifanov V. V., Soldatov A. Ju., Soldatov E. Ju., Podlegaev A. P., Skorikov V. S. Metod ocenivanija riskov v sistemah prinjatija reshenij s uchetom zashhity informacii. Vestnik SibGUTI. 2023; 17(2). s. 84–92.
25. Ermakov S. A., Chursin A. G., Bolgov A. A. Nechetko-mnozhestvennaja metodika ocenki riskov avtomatizirovannoj sistemy «Umnyj dom» s dinamicheskoj topologiej Informacija i bezopasnost'. 2022, Tom: 25, № 4, s. 495–500.
26. Ermakov S. A., Bolgov A. A. Ocenka riska s ispol'zovaniem nejro-nechetkoj sistemy // Informacija i bezopasnost'. 2022, Tom: 25, № 4, s. 583–592.
27. Ermakov S. A., Gusareva Ju. A., Bolgov A. A., Kostrova V. N. Povyshenie zashhishhennosti avtomatizirovannoj sistemy «umnyj dom»: algoritm ocenki riskov narushenija konfidencial'nosti informacii // Informacija i bezopasnost'. 2022, Tom: 25, № 3, s. 377–388.
28. Kosmacheva I. M., Davidjuk N. V., Sibikina I. V., Kuchin I. Ju. Model' ocenki jeffektivnosti konfiguracii sistemy zashhity informacii na baze geneticheskih algoritmov // Modelirovanie, optimizacija i informacionnye tehnologii. 2020; 8(3). Dostupno po: https://moit.vivt.ru/wp-content/uploads/2020/08/KosmachevaSoavtors_3_20_1.pdf DOI: 10.26102/2310-6018/2020.30.3.022.
29. Semenov V. V. Ocenivanie sostojanija informacionnoj bezopasnosti na osnove analiza vremennyh rjadov // Nauchno-tehnicheskij vestnik Povolzh'ja. 2021, № 10, s. 127–129.
30. Rychkova A. A., Bur'kova E. V., Konnov A. L. Analiz ugroz informacionnoj bezopasnosti na osnove metoda klasterizacii dannyh // Nauchno-tehnicheskij vestnik Povolzh'ja. 2023, № 6, s. 307–310.
31. Promyslov V. G., Akimov N. N., Abdulova E. A., Golubev P. A., Zharko E. F., Zhmajlov V. V., Lepehin I. Ju., Lobanok O. I., Ishakov A. Ju., Meshherjakov R. V., Poletykin A. G., Musihin A. M., Pronin V. V., Semenkov K. V., Cyrenov D. V. Ocenka riska i obespechenie kiberbezopasnosti atomnyh jelektrostancij. M.: IPU RAN, 2022. – 193 s.
32. Zharko E. F., Promyslov V. G., Ishakov A. Ju., Meshherjakov R. V., Semenkov K. V., Abdulova E. A., Bajbulatov A. A., Ishakov S. Ju. Kiberbezopasnost' bespilotnyh transportnyh sredstv. Arhitektura. Metody proektirovanija. M.: Radiotehnika, 2021. – 160 s.
33. Vetrov I. A., Podtopel'nyj V. V. Osobennosti formirovanija vektora sovremennyh setevyh atak. Vestnik SibGUTI. 2022, № 3, s. 3–13.
34. Meshherjakov R. V., Ishakov A. Ju., Evsjutin O. O. Sovremennye metody obespechenija celostnosti dannyh v protokolah upravlenija kiberfizicheskih sistem. Informatika i avtomatizacija. 2020, 19(5), s. 1089–1122.
35. Bukin A. V., Samonov A. V., Tihonov Je. I. Obnaruzhenie incidentov informacionnoj bezopasnosti na osnove tehnologii nejronnyh setej // Voprosy kiberbezopasnosti. 2022, № 5(51), s. 61–73.
36. Saenko I. B., Kotenko I. V., Al'-Barri M. H. Primenenie iskusstvennyh nejronnyh setej dlja vyjavlenija anomal'nogo povedenija pol'zovatelej centrov obrabotki dannyh // Voprosy kiberbezopasnosti. 2022, № 2(48), s. 87–97.
37. Merkal'do F., Martinelli F., Santone A. Proverka modeli dlja obnaruzhenija atak v real'nom vremeni v sistemah raspredelenija vody. Informatika i avtomatizacija. 2022, 21(2), s. 219–242.
38. Shtyrkina A. A. Metod rekonfiguracii topologii kiberfizicheskoj sistemy na osnove grafovoj iskusstvennoj nejronnoj seti // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2023, 2 (54), s. 173–182.
39. Sergadeeva A. I., Lavrova D. S. Primenenie modul'noj nejronnoj seti dlja obnaruzhenija DDOS-atak // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy 2023, № 1 (53), s. 111–118.
40. Aleksandrova E. B., Shtyrkina A. A. Metod adaptivnoj nejtralizacii strukturnyh narushenij kiberfizicheskih sistem na osnove grafovyh iskusstvennyh nejronnyh setej // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2023, № 4 (52), s. 89-100.
41. Car'kova E. G. K voprosu primenenija iskusstvennyh nejronnyh setej v sistemah obespechenija transportnoj bezopasnosti // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2022, Tom: 3, № 3 (3), s. 28–34.
42. Kubasov I. A., Sushkov V. I. Primenenie tehnologij iskusstvennogo intellekta v robototehnicheskih kompleksah special'nogo naznachenija v celjah obespechenija pravoohranitel'noj dejatel'nosti // Vestnik Voronezhskogo instituta FSIN Rossii. 2022, № 3, s. 69–76.
43. Alekseenko S. P., Dostov V. V. Nejroseti i informacionnaja bezopasnost' v pravoohranitel'nyh strukturah // Ohrana, bezopasnost', svjaz'. 2022, № 7-2, s. 11–16.
44. Ataki na iskusstvennyj intellekt. Kak zashhitit' mashinnoe obuchenie v sistemah bezopasnosti. Aleksandr Chistjakov, Aleksej Andreev «Laboratorija Kasperskogo», Departament issledovanija ugroz. https://media.kaspersky.com/ru/business-security/attacks-on-artificial-intelligence-whitepaper.pdf
45. Kotenko I. V., Saenko I. B., Lauta O. S., Kribel' A. M. Metodika obnaruzhenija anomalij i kiberatak na osnove integracii metodov fraktal'nogo analiza i mashinnogo obuchenija. Informatika i avtomatizacija, 2022, 21(6), s. 1328–1358.
46. Zegzhda D. P., Kalinin M. O., Krundyshev V. M., Lavrova D. S., Moskvin D. A., Pavlenko, E. Ju. Primenenie algoritmov bioinformatiki dlja obnaruzhenija mutirujushhih kiberatak // Informatika i avtomatizacija, 2021, 20(4), s. 820–844.
47. Kalinin M. O., Tkacheva E. I. Decentralizovannyj podhod k obnaruzheniju vtorzhenij v dinamicheskih setjah interneta veshhej na baze mnogoagentnogo obuchenija s podkrepleniem i mezhagentnym vzaimodejstviem // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2023, № 2 (54), s. 202–211.
48. Kalinkin A. O. i dr. Obnaruzhenie programm-shifroval'shhikov na osnove dannyh mehanizma trassirovki sobytij i primenenija metoda mashinnogo obuchenija // Bezopasnost' informacionnyh tehnologij. 2022, t. 29, № 3, s. 82–93.
49. Sinjuk A. D., Ostroumov O. A., Tarasov A. A. (). Teoretiko-informacionnoe predstavlenie virtualizacii setevogo kanala perehvata // Informatika i avtomatizacija. 2023, 22(4), s. 721–744.

50. *Makarova O. S., Porshnev S. V. Ocenivanie verojatnostej komp'juternyh atak na osnove funkcij // Bezopasnost' informacionnyh tehnologij. 2020, t. 27, № 2, s. 86-96.*
51. *Markov G. A., Krundyshev V. M., Kalinin M. O., Zegzhda D. P., Busygin A. G. Obnaruzhenie komp'juternyh atak v setjah promyshlennogo interneta veshhej na osnove vychislitel'noj modeli ierarhicheskoj vremennoj pamjati // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2023, № 2 (54), s. 163–172.*
52. *Meshherjakov R. V., Ishakov S. Ju. Issledovanie indikatorov komprometacii dlja sredstv zashhity informacionnyh i kiberfizicheskih sistem // Voprosy kiberbezopasnosti. 2022, № 5 (51), s. 82–99.*
53. *Pavlova K. S. Primenenie predmetnyh ontologij v oblasti obespechenija bezopasnosti informacii // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2023, Tom: 1, № 1 (1), s. 24–29.*
54. *Ruchaj A. N., Tokarev I. V., Gribachjov A. S. Metody mashinnogo obuchenija i iskusstvennogo intellekta v sfere informacionnoj bezopasnosti: analiz sovremennogo sostojanija i perspektivy razvitija // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2022, 4 (46), s. 76–87.*
55. *Artamonov V. A., Artamonova E. V., Safonov A. E. Bezopasnost' iskusstvennogo intellekta // Zashhita informacii. Insajd. 2022, № 6 (108), s. 8–17.*
56. *Artamonov V. A., Artamonova E. V. Iskusstvennyj intellekt v sistemah bezopasnosti // Zashhita informacii. Insajd. 2022, № 5 (107), s. 40–49.*
57. *Lebedev I. S., Suhoparov M. E. Ispol'zovanie informacii o vlijajushhih faktorah dlja razbienija vyborok dannyh v metodah mashinnogo obuchenija dlja ocenki sostojanija IB // Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2023, №2 (54), s. 125–134.*
58. *Sarker I., Kayes A., Badsha S., Alqahtani H., Watters P., Ng A. Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 2020.*
59. *Musser M., Garriott A. Machine Learning and Cybersecurity. Center for Security and Emerging Technology, 2021.*
60. *Chekmarev M. A., Kljuev S. G., Bobrov N. D. Analiz metodov obespechenija bezopasnosti sistem mashinnogo obuchenija. Modelirovanie, optimizacija i informacionnye tehnologii. 2022; 10(1). DOI: 10.26102/2310-6018/2022.36.1.006*
61. *Evsutin O., Melman A., Meshcheryakov R. Digital steganography and watermarking for digital images: a review of current research directions IEEE Access. 2020, Vol. 8, pp. 166589–166611.*
62. *Horev A. A. Nekotorye podhody k ocenke vozmozhnostej perehvata pobochnyh jelektromagnitnyh izluchenij sredstv vychislitel'noj tehniki, ispol'zujushhih cifrovye interfejsy // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2022, № 3 (45), s. 5–16.*
63. *Sychev M. P., Mazin A. V., Zelencova E. V., Krylov V. O., Sidel'nikov A. P. Funkcional'nye aspekty modelirovanija processa perehvata informativnyh signalov po parametricheskim kanalam // Pribory i sistemy. Upravlenie, kontrol', diagnostika. 2022, № 2, s. 22–33.*
64. *Sychev M. P., Nikulin S. S., Man'kov E. A. Perehvat informacii po parametricheskim kanalam: strukturizacija funkcional'nogo predstavlenija jetapa obrabotki perehvachennyh informativnyh signalov s cel'ju formirovanija celostnogo ob#ema informacii ob ob#ekte razvedki // Vestnik Voronezhskogo instituta MVD Rossii. 2023, № 2, s. 87–93.*
65. *Meshherjakov R. V., Los' V. P., Shherbakov V. A., Rekunkov I. S. Matematicheskoe modelirovanie zashhitnyh jekranov dlja predotvrashhenija utechki informacii po tehnicheskim kanalam v radiodiapazone // Voprosy zashhity informacii. 2023, № 1 (140), s. 47–52.*
66. *Kopytov P. D., Koroljov I. D., Kulish O. A., Stepancov S. V. Postroenie formal'nyh modelej rasprostranenija pobochnyh jelektromagnitnyh izluchenij po tehnicheskim kanalam utechki informacii dlja ob#ektov vychislitel'noj tehniki ot tehnicheskih sredstv razvedki // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2023, № 1 (47), s. 102–111.*
67. *Zaharov A. V. Trebovanija k sovremennomu programmno-apparatnomu kompleksu radiokontrolja i cifrovogo analiza signalov // Zashhita informacii. Insajd. 2022, № 1 (103), s. 24–33.*
68. *Alekseenko S. P., Antilikatorov A. B., Astahov N. V. Metodika vybora modeli ohrany ob#ekta radiotehnicheskimi sredstvami obnaruzhenija // Vestnik Voronezhskogo instituta MVD Rossii. 2023, № 1, s. 57–62.*
69. *Aver'janov A. A., Shadriv V. V., Berdjugin V. Ju. Matematicheskaja model' ocenki ugroz fizicheskogo proniknovenija zloumyshlennika na zashhishhennyj ob#ekt // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2022, № 4 (46), s. 52–57.*
70. *Jazov Ju. K., Solov'ev S. V., Tarelkin M. A. Primenenie sostavnyh setej Petri-Markova pri matematicheskom modelirovanii ugroz bezopasnosti informacii // Ohrana, bezopasnost', svjaz'. 2023, № 8–2, s. 185–196.*
71. *Avsent'ev A. O. Problema postroenija mnogoagentnyh sistem zashhity informacii na ob#ektah informatizacii ot utechki po tehnicheskim kanalam // Vestnik Voronezhskogo instituta MVD Rossii. 2022, № 3, s. 68–77.*
72. *Kalach A. V., Zdol'nik V. V. Matematicheskaja model' pokazatelja jeffektivnosti mer, napravlennyh na predotvrashhenie utechki informacii po kanalam pobochnyh jelektromagnitnyh izluchenij i navodok. Vestnik Voronezhskogo instituta FSIN Rossii. 2022, № 1, s. 54-61.*
73. *Minaev V. A., Korobec B. N., Sychev M. P., Sevrjukov D. V., Dudoladov V. A. Kljuchevye funkcional'nye pokazateli radiotehnicheskih sredstv obnaruzhenija proniknovenija na ohranjaemye ob#ekty // Voprosy oboronnoj tehniki. Serija 16: Tehnicheskie sredstva protivodejstvija terrorizmu. 2019, № 5–6 (131-132), s. 3–7.*
74. *Alekseev D. S., Kozlov R. S. Metod prakticheskoj ocenki jeffektivnosti sredstv aktivnoj zashhity ot utechki konfidencial'noj informacii po tehnicheskomu kanalu // Nauchno-tehnicheskij vestnik Povolzh'ja. 2023, № 4, s. 201–204.*
75. *Bur'kova E. V., Rychkova A. A. Metodika prinjatija reshenij pri vybore sredstv fizicheskoj zashhity na osnove metoda analiza ierarhii // Nauchno-tehnicheskij vestnik Povolzh'ja. 2021, № 5, s. 119–123.*
76. *Avsent'ev O. S., Val'de A. G. Verbal'naja model' zashhity informacii ot utechki po tehnicheskim kanalam v processe formirovanija sistemy zashhity informacii na ob#ektah informatizacii // Vestnik Voronezhskogo instituta MVD Rossii. 2022, № 2, s. 18–27.*
77. *Pantjuhov D. V., Loginov I. V. Varianty postroenija intellektual'nyh sistem fizicheskoj bezopasnosti s uchetom razvitija tehnologij intellektualizacii // Ohrana, bezopasnost', svjaz'. 2023, № 8-1, s. 155–159.*
78. *Kostogryzov A. I. Podhod k verojatnostnomu prognozirovaniju zashhishhennosti reputacii politicheskih dejatelej ot «fejkovyh» ugroz v publichnom informacionnom prostranstve // Voprosy kiberbezopasnosti. 2023, № 3 (55), s. 114–133*
79. *Avetisjan A. I. Ispol'zovanie doverennogo PO pri sozdanii sistem iskusstvennogo intellekta kak osnova bezopasnosti (doklad) // XXVII nauchno-prakticheskaja konferencija «Kompleksnaja zashhita informacii», 24–26 maja 2022 goda, Moskovskaja oblast'.*
80. *Garbuk S. V. Zadachi normativno-tehnicheskogo regulirovanija intellektual'nyh sistem informacionnoj bezopasnosti // Voprosy kiberbezopasnosti. 2021, № 3 (43), s. 68–83.*