Применение систем искусственного интеллекта в защите информации

Шананин Василий Андреевич
старший преподаватель, ИСТАС, Московский государственный строительный университет (МГСУ),
shananinva.infonom@gmail.com

Статья посвящена рассмотрению и анализу основные направлений применения искусственного интеллекта в области информационной безопасности. Отмечается, что повсеместное внедрение интеллектуальных систем обусловлено информатизацией и виртуализацией общества, а также ростом количества киберугроз, увеличения их сложности и разнообразия. Автор статьи отмечает, что для того, чтобы искусственный интеллект смог обеспечить требуемый уровень защиты информации, он должен быть корректно имплементирован, интегрирован в существующие системы и обучен. При этом, само по себе введение в эксплуатацию интеллектуальных систем, призванных защищать данные, может привести к колоссальной по масштабу последствий «бреши» в системе защиты и существенно снизить уровень безопасности индивидуального или корпоративного пользователя. Рассмотрены проблемы, возникающие при обучении и вводе в эксплуатацию интеллектуальной системы (privacy breach, data poisoning, evasion attack и проч. В данной связи рассмотрена категория «надежный искусственный интеллект» (Trusted Artificial Intelligence). Обзор существующей литературы и практик применения искусственного интеллекта позволил автору определить и представить в статье наиболее перспективные виды «умных» систем. Рассмотрен отдельный прикладной вектор имплементации интеллектуального интеллекта в защите информации – борьба со спуфингом; рассмотрены типы интеллектуальных методов защиты от спуфинга голосовой аутентификации, применяемых на современном этапе. Автор, помимо прочего, определяет перспективные пути развития методов биометрического сканирования, основанных на интеллектуальных алгоритмах и Behavioral Biometrics в частности.
Ключевые слова: искусственный интеллект, информационная безопасность, цифровая экономика, голосовая аутентификация, биометрические данные, киберпреступность

Технологии искусственного интеллекта постепенно входят во все сферы функционирования общества и государства. Многообразие данных технологий уже сейчас позволяет говорить о практически неограниченном спектре решаемых ими задач. ***Интеллектуализация общества***, ***власти и бизнеса*** имеет место и в нашей стране: в 2019 г., в частности, была утверждена «Национальная стратегия развития искусственного интеллекта на период до 2030 года», в тексте которой искусственный интеллект позиционируется в качестве единственно возможно пути развития «цифрового государства» [3, с. 109]. В научных кругах речь все чаще идет о внедрении в ту или иную сферу не одной, а сразу нескольких интеллектуальных систем, объединенных в единую гибридную среду (концепция «мягких вычислений»), позволяющую добиться синергетического эффекта от применения каждой из используемых технологий [6, с. 48].

Еще одной важной тенденцией развития общества является его ***информатизация***: современный человек живет не только в мире реальном, но и в мире виртуальном; люди все чаще доверяют компьютерам важную персональную, финансовую, социальную, медицинскую информацию. Все это актуализирует вопросы обеспечения информационной безопасности на всех уровнях функционирования общественной системы – индивидуальном, групповом, корпоративном, государственном. В современном мире «люди ищут способы крепко и, главное, надежно закрыть данные от других – будь то аккаунт в социальной сети или стратегически важный военный объект» [2, с. 393].

Количество киберугроз обнаруживает постоянный рост; увеличивается их сложность и разнообразие. По данным О. М. Махалиной и В. Н. Махалина, затраты среднего бизнеса на ликвидацию последствий одного киберинцидента в России составляют около 1,6 млн руб.; крупные компании тратят в этих целях порядка 16,1 млн руб [11, с. 134]. Угрозы информационной безопасности можно понимать как совокупность действий и факторов, создающих риск нанесения ущерба национальным, корпоративным и персональным интересам в информационной сфере [11, с. 135]. Озабоченность мировой общественности по поводу защиты информации привела к утверждению ряда межгосударственных регламентов по защите данных; отметим, к примеру, «Общие правила защиты данных (GDPR)» (2018 г.), которые предписывают обеспечивать строгое соответствие компьютерных систем принципам работы с персональной и корпоративной информацией [4, с. 92].

Сочетание двух параллельных тенденций породило массу дискуссий о том, ***могут ли системы, основанные на искусственном интеллекте, выступать в качестве действенных инструментов защиты информации***. Споры о прикладном значении систем искусственного интеллекта в области информационной безопасности ведутся в течение последнего десятиле-

тия, но на рынок данные инструменты вышли относительно недавно – тогда, когда «зрелость таких продуктов позволила применять их в корпоративных средах», а эффективность их работы стала оправдывать их стоимость. Кроме того, возможности киберпреступников растут пропорционально увеличению степени технологизации общества (или даже быстрее), поэтому противостоять правонарушителям в «ручном» режиме сегодня, пожалуй, невозможно, в связи с чем и получают распространение защитные системы искусственного интеллекта. На текущий момент очевидно, что технологии искусственного интеллекта способны проводить оперативный и точный анализ систем безопасности и идентифицировать возможность уязвимостей; более того, такие системы могут формировать банк данных об уязвимостях и обучаться знаниям о них, автоматически реагировать на угрозы и кибератаки [9, с. 116].

Релевантность искусственного интеллекта в информационной безопасности можно подтвердить макроэкономическими показателями: уже к 2019 г. мировой рынок технологий искусственного интеллекта, применяемых в сфере информационной безопасности, достиг оценочного показателя в $8 млрд, а к 2025 г. он, согласно экспертным прогнозам, вырастет до $30 млрд или более [12].

При этом нельзя сказать, что современные методологии защиты данных посредством искусственного интеллекта совершенны. Напротив, разработчики соответствующего ПО все чаще говорят о необходимости существенного улучшения применяемых систем. Рассмотрим в качестве примеров некоторые важные проблемные области развития искусственного интеллекта, направленного на защиту данных. Во-первых, самообучающаяся система должна различать отклонения в поведении пользователей, но при этом идентифицировать их в качестве таковых. Речь идет о том, что алгоритмы машинного обучения должны отличать намеренно введенные вредоносные данные от реальных аномальных событий. Во-вторых, искусственный интеллект должен самостоятельно выявлять конфиденциальную информацию, даже если пользователь не классифицирует ее таковой. Клиент может предоставить доступ к закрытой информации неосознанно, ненамеренно, случайно [10].

Для того, чтобы искусственный интеллект смог обеспечить требуемый уровень защиты информации, он должен быть корректно имплементирован, интегрирован в существующие системы и обучен. Парадоксально, но ***само по себе введение в эксплуатацию интеллектуальных систем, призванных защищать данные, может привести к колоссальной по масштабу последствий «бреши» в системе защиты и существенно снизить уровень безопасности индивидуального или корпоративного пользователя***.

Одной из проблем, возникающих при обучении и вводе в эксплуатацию интеллектуальной системы, может стать нарушение конфиденциальности (*privacy breach*). В данной связи фокус внимания смещается на новые технологии повышения конфиденциальности; к примеру, технология *OPAL* (*open algorithms project*) позволяет отказаться от пересылки данных алгоритму искусственного интеллекта за счет предоставления удаленного и контролируемого доступа к информации.

Сценарием, сопряженным с максимальной степенью риска для системы безопасности, считается так называемое отравление данных (*data poisoning*). Отравление данных имеет место в ситуации обучения нейросети, когда ей предлагается ложная информация, искажающая обучающую выборку, что, таким образом, приводит к обесцениванию результатов обучения. Нейросеть при этом по завершении обучения будет обучена принимать неверные решения, выгодные третьим сторонам; масштаб ущерба от подобной манипуляции может быть крайне вариативным – от репутационного ущерба конкретной личности до изменения электорального поведения широких масс. Несмотря на то, что современная научная литература содержит описание ряда моделей для борьбы с отравлением данных, ни одна из подобных моделей еще не прошла полноценное апробирование в реальной практике.

Схожей проблемой является атака уклонения (*evasion attack*), имеющая место в ситуации применении искусственного интеллекта [13, с. 27]. Третья сторона, незаметно для системы и лица, контролирующего ее работу, видоизменяет входные значения, которые в результате приводят к порождению некорректных умозаключений со стороны самой системы. В качестве единственного эффективного метода противодействия данному виду угроз называют состязательную тренировку (*adversarial training*), позволяющую на этапе обучения обучить систему не включать в аналитическую выборку ложные данные и классифицировать их в качестве информационных помех [1, с. 68].

Многие системы искусственного интеллекта уже успели скомпрометировать себя, и поэтому не всегда понятно, когда и каким образом следует имплементировать «умную» систему в процессе защиты данных. С. М. Авдошин и Е. Ю. Песоцкая в данной связи вполне обоснованно оперируют термином «надежный искусственный интеллект» (*Trusted Artificial Intelligence*), интерпретируя его как совокупность систем, сконструированных на основе принципа доверия; систем, в которых исключены риски злоупотребления возможностями искусственного интеллекта со стороны владельцев технологий; систем, результатам работы которых можно доверять [1, с. 63].

Использование инструментов, основанных на искусственном интеллекте, обусловлено, во-первых, ***необходимостью оперативного реагирования при наступлении ситуации уязвимости системы защиты информации*** и, во-вторых, ***нехваткой квалифицированных специалистов***. В идеальной ситуации в компании должна работать круглосуточная служба информационной безопасности – для того, чтобы обеспечить защиту в нерабочее время. Более того, непосредственно перед атакой киберпреступники зачастую реализуют «отвлекающие маневры», активируя DDoS-атаку или сетевое сканирование, что может отвлечь специалистов и «перетянуть» рабочие ресурсы на противодействие подобным предварительным атакам [5, с. 152]. В данной связи все большее число компаний обращаются к интеллектуальным ресурсам защиты данных, которые способны обрабатывать большое количество событий, автоматизировать действия аналитиков и обеспечивать оперативное реагирование. Вышеизложенное позволяет нам говорить и о третьем факторе, влияющем на распространение интеллектуальных систем защиты данных. Речь идет о том, что ***современная киберпреступность использует интеллектуальные системы, следовательно, бороться с ней можно используя лишь симметричные по уровню техноло-***

гичности меры. С. М. Авдошин и Е. Ю. Песоцкая указывают, что в современных условиях «цифровой диктатуры» (*digital dictatorship*) цифровая защита и борьба с недобросовестным использованием информации – приоритет «цифровых» стратегий любого общества [1, с. 63].

Классические интеллектуальные системы сконструированы на основе анализа отклонений: превышение объема специфического трафика, неуспешные попытки аутентификации, паттерны (признаки, шаблоны) работы пользователей, идентификация скомпрометированных учетных записей. Обзор существующей литературы и практик применения искусственного интеллекта позволяет определить наиболее перспективные виды «умных» систем.

Средства *EDR* (*Endpoint Detection and Response*) представляют собой платформы обнаружения атак на рабочих станциях, серверах, компьютерных устройствах и оперативного реагирования на них. Технологии искусственного интеллекта данного типа способны идентифицировать вредоносные программы, классифицировать угрозы и автономно реагировать на них, компилируя при этом отчетность по выявленным и нейтрализованным угрозам. Система в данном случае принимает решение на основании анализа базы данных, собранной со множества устройств (так называемых «конечных точек») [12].

Средства защиты приложений (*Application Security*) в качестве «конечных точек» используют не устройства, а приложения (что, собственно, значительно ограничивает сферу их применения); тем не менее, такие системы вполне успешно используются во всем мире благодаря высокой эффективности самообучаемости, адаптивности риск-моделей, тщательному сканированию систем безопасности [12].

NDR (*Network Detection and Response*) работает преимущественно не с «конечными точками», а выявляют угрозы безопасности данных еще на сетевом уровне. Продукты данного типа выявляют угрозы в сетевом трафике и автоматически реагируют на них посредством изменения конфигурации сетевых устройств и шлюзов.

UEBA (*User and Entity Behavior Analytics*) представляет собой систему поведенческого анализа пользователей. Нестандартный паттерн позволяет классифицировать аномальные действия пользователя в качестве угрозы. Аномальное поведение приводит к блокировке пользователя, ограничению его доступа к сетевому ресурсу; подобный инструментарий доказал свою эффективность в защите конфиденциальных данных, при проверках соблюдения регламентов и нормативных актов [12].

TIP (*Threat Intelligence Platform*) представляет собой группу инструментов ранней идентификации угроз и реагирования на них; алгоритмы *TIP* функционируют на базисе большого количества различных данных (*Data Lake*) и индикаторов компрометации (*IoC*). Особенностью и преимуществом подобных средств является возможность идентификации угроз еще до момента ее взаимодействия с пользовательской системой, т. е. на самом раннем этапе, во внешней среде.

Механизм работы инструментов *SIEM* (*Security Information and Event Management*) и *SOAR* (*Security Orchestration and Automated Response*) весьма схож с вышеописанным, однако отличается возможностью применения эвристических методов в анализе данных о внешней среде [12], что, в свою очередь, сокращает количество ложных срабатываний при обнаружении аномальных паттернов.

Отдельным и весьма значимым прикладным вектором имплементации интеллектуального интеллекта в защите информации является борьба со спуфингом. Спуфинг (*spoofing attack*) – крайне распространенная в цифровом мире противоправная деятельность, направленная на выполнение сфальсифицированной аутентификации в системе (как правило, речь в данном случае идет об аутентификации посредством биометрических данных и голосового ввода) [8, с. 91]. Злоумышленник, проникнув в чужой аккаунт, получает нужный ему сегмент личных или корпоративных данных для последующего использования. Абсолютное большинство контрмер против спуфинга основывается именно на системах искусственного интеллекта.

Методы защиты данных от спуфинга направлены, в первую очередь, на противодействие фальсификации голосовых данных человека. Голосовая аутентификация набирает сегодня колоссальную популярность по причинам легкости в использовании и оперативности. Возникновение широкого спектра умных устройств и эволюция интернета вещей (*IoT*) привели к тому, что голосовой интерфейс стал практически таким же востребованным, как визуальный. По собранной на 2022 г. статистике, около 500 миллионов пользователей ежемесячно используют *Google Assistant*; голосовой помощник *Siri* обрабатывает 25 миллиардов запросов ежемесячно [8, с. 85]. Голосовые помощники входят к обиход многих людей, они используются при управлении автомобилями, умными домами, применяются в платёжных системах и банкинге. Рост потребительской ценности «голосовых платежей» стимулирует платёжных провайдеров (*PayPal, Amazon, Apple* и *Google*) развивать технологий искусственного интеллекта, направленные на обработку голоса. При этом ***ключевым барьером для массового внедрения голосовой аутентификации являются вопросы проблемы информационной безопасности и учащение случаев спуфинга*** [2, с. 396].

Рассмотрим типологию интеллектуальных методов защиты от спуфинга голосовой аутентификации, применяемых на современном этапе:

1. Интерактивная аутентификация. Для того, чтобы доступ в систему был каждый раз защищен новым, уникальным, нерегулярным паролем, были представлены интеллектуальные системы, подразумевающие не точечный ввод идентификационных данных, а так называемую динамическую аутентификацию. Пользователь должен взаимодействовать с системой непосредственно в процессе аутентификации (к примеру, искусственный интеллект генерирует случайный текст, который должен вслух прочитать пользователь, а затем полученная аудиозапись подвергается мультифакторному интеллектуальному анализу и проверке на подлинность).

2. Идентификация сгенерированного или синтезированного голоса. Подобная контрмера реализуется посредством извлечения из голосовой записи разного рода дефектов и помех, свидетельствующих о синтетической природе голоса на записи. Роботизированные самообучающиеся системы на текущий момент вполне успешно работают на базисе интеграции ряда методо-

логий: анализа кратковременных спектральных характеристик, построения модели гауссовой смеси, алгоритмов опорных векторов, нейронных сетей.

3. Идентификация сгенерированного или синтезированного голоса на базисе артикуляционной специфики человека. Подобные контрмеры опираются на характерные помехи и эффекты, создаваемые речевым трактом человека. Естественные шумы достаточно сложно воспроизвести искусственно, что позволяет эффективно идентифицировать искусственную речь [8, с. 91].

Таким образом, крупные производители аппаратных средств все активнее заменяют скомпрометированную связку «логин – пароль» более прогрессивной процедурой аутентификации, и голосовая аутентификация является одной из подобных альтернатив. Помимо него, широко распространены прочие ***методы биометрического сканирования, основанные на интеллектуальных алгоритмах***. При этом область биометрии сейчас находится в фазе трансформации – идет поиск более совершенных «умных» способов сбора данных и вырабатываются новые системы защиты от их фальсификации. К примеру, перспективным на сегодняшний день является такой метод, как *Behavioral Biometrics* (поведенческая биометрия). Искусственный интеллект не просто умеет распознавать голос, отпечаток пальца или лицо пользователя, а анализирует специфику его активности: клавиатурный почерк, особенности движений при работе с мышью, сенсорной панелью. Важным преимуществом поведенческой биометрии в сравнении с традиционным биометрическим сканированием статичных параметров является то, что отслеживание аутентичности предусмотрено в *Behavioral Biometrics* в непрерывном режиме, в процессе работы пользователя с устройством. Постепенно в массовую практику переходят интеллектуальные систем поведенческой биометрии, которые способны фиксировать особенности походки, стиля одежды, интерьеров, дыхательные характеристики и динамику показателей сердцебиения [7, с. 140].

Таким образом, мы живем в эпоху, когда центральной проблемой для пользователей, бизнес-структур и регулирующих органов стала проблема защиты персональных данных. Пользователи требуют обеспечения большей прозрачности и контроля в области сбора, хранения и использования данных, а также обмена данными. Защита информации стала одной из приоритетных задач, стоящих перед обществом. Вопрос защиты информации актуален как никогда ранее, так как масштабы киберпреступности постоянно растут. Один из возможных инструментов противодействия киберугрозам – технологии искусственного интеллекта. Большинство современных решений в сфере информационной безопасности так или иначе основаны на искусственном интеллекте. При этом внедрение искусственного интеллекта в область защиты информации сопряжено с массой рисков, в связи с чем специалисты в области обработки данных объединяют свои усилия для разработки инструментов защиты персональных данных для систем искусственного интеллекта, которые появятся в недалеком будущем.

Литература

1. Авдошин, С. М. Доверенный искусственный интеллект как способ цифровой защиты / С. М. Авдошин, Е. Ю. Песоцкая // Бизнес-информатика. – 2022. – №2. – С. 62-73.
2. Алиев, А. Системы защиты биометрических данных / А. Алиев, М. З. К. Мусаева // Academic research in educational sciences. – 2021. – №4. – С. 393-396.
3. Арутюнов, В. В. Применение методов искусственного интеллекта для обеспечения информационной безопасности: результативность и востребованность итогов исследований российских учёных / В. В. Арутюнов // Научные и технические библиотеки. – 2020. – № 11. – С. 105-116.
4. Асеева, И. А. Искусственный интеллект и большие данные : этические проблемы практического использования. (аналитический обзор) / И. А. Асеева // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 8, Науковедение: Реферативный журнал. – 2022. – №2. – С. 89-98.
5. Афанасьева, Д. В. Применение искусственного интеллекта в обеспечении безопасности данных / Д. В. Афанасьева // Известия ТулГУ. Технические науки. – 2020. – №2. – С. 151-154.
6. Васильев, В. И. Применение методов искусственного интеллекта в задачах защиты информации (по материалам научной школы УГАТУ) / В. И. Васильев, В. М. Картак // Системная инженерия и информационные технологии. – 2020. – Т. 2, № 2 (4). – С. 43-50.
7. Довгаль, В. А. Анализ перспективных методов поведенческой биометрии для аутентификации пользователей / В. А. Довгаль, Д. В. Довгаль // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2017. – №3 (206). – С. 139-142.
8. Евсюков, М. В. Методы защиты в современных системах голосовой аутентификации / М. В. Евсюков, М. М. Путято, А. С. Макарян, В. О. Немчинова // Прикаспийский журнал: управление и высокие технологии. – 2022. – №3 (59). – С. 84-92.
9. Литвин, И. И. Особенности сбора, обработки и защиты персональных данных искусственным интеллектом / И. И. Литвин // Вестник Уральского юридического института МВД России. – 2021. – №4. – С. 112-118.
10. Маршалл, Э. Безопасность искусственного интеллекта и машинного обучения: перспективы в корпорации Майкрософт / Э. Маршалл, Р. Рохас, Д. Стоукс, Д. Бринкман // Microsoft. – 2022 [Электронный ресурс]. – Режим доступа: https://learn.microsoft.com/ru-ru/security/engineering/securing-artificial-intelligence-machine-learning. – Дата доступа: 15.11.2022.
11. Махалина, О. М. Цифровизация бизнеса увеличивает затраты на информационную безопасность / О. М. Махалина, В. Н. Махалин // Управление. – 2020. – №1. – С. 134-140.
12. Шабанов, А. Применение технологий искусственного интеллекта в информационной безопасности / А. Шабанов // AM Live. – 2022 [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/analytics/Technology_Analysis/using-artificial-intelligence-technologies-in-information-security. – Дата доступа: 15.11.2022.
13. Moldamurat, K. Intelligent mechanism of hinding cryptographically protected communication channel / K. Moldamurat, D. Kalmanova, D. Yergaliyev, T. Beybithan // НиКа. – 2018. – №. 2. – С. 25-26.

Application of artificial intelligence systems in information protection

Shananin V.A.
Moscow State University of Civil Engineering (MGSU)

JEL classification: C10, C50, C60, C61, C80, C87, C90

The article is devoted to the consideration and analysis of the main areas of application of artificial intelligence in the field of information security. It is noted that the widespread introduction of intelligent systems is due to the informatization and virtualization of society, as well as an increase in the number of cyber threats, an increase in their complexity and diversity. The author of the article notes that in order for artificial intelligence to be able to provide the required level of information protection, it must be correctly implemented, integrated into existing systems and trained. At the same time, the mere introduction of intelligent systems designed to protect data can lead to a colossal “breach” in the protection system and significantly reduce the level of security of an individual or corporate user. The problems that arise during the training and commissioning of an intelligent system (privacy breach, data poisoning, evasion attack, etc.) are considered. In this regard, the category of Trusted Artificial Intelligence is considered. A review of the existing literature and practices of using artificial intelligence allowed the author identify and present in the article the most promising types of smart systems. A separate application vector of the implementation of intellectual intelligence in information security is considered - the fight against spoofing; the types of intelligent methods for protecting against spoofing voice authentication used at the present stage are considered. The author, among other things, identifies promising ways of developing biometric scanning methods based on intelligent algorithms and Behavioral Biometrics in particular.
Keywords: artificial intelligence, information security, digital economy, voice authentication, biometric data, cybercrime

References

1. Avdoshin, S. M. Trusted artificial intelligence as a way of digital protection / S. M. Avdoshin, E. Yu. Pesotskaya // Business Informatics. - 2022. - No. 2. - S. 62-73.
2. Aliev, A. A. Aliev, M. Z. K. Musaeva, Biometric data protection systems // Academic research in educational sciences. - 2021. - No. 4. – S. 393-396.
3. Arutyunov, V. V. Application of artificial intelligence methods to ensure information security: the effectiveness and demand for the results of research by Russian scientists / V. V. Arutyunov // Scientific and technical libraries. - 2020. - No. 11. - C. 105-116.
4. Aseeva, I. A. Artificial intelligence and big data: ethical problems of practical use. (analytical review) / I. A. Aseeva // Social and humanitarian sciences. Domestic and foreign literature. Ser. 8, Science of Science: Abstract Journal. - 2022. - No. 2. – S. 89-98.
5. Afanas'eva, D. V. The use of artificial intelligence in data security / D. V. Afanas'eva // Izvestiya TulGU. Technical science. - 2020. - No. 2. - S. 151-154.
6. Vasiliev, V. I. Application of artificial intelligence methods in information security problems (based on the materials of the scientific school of the USATU) / V. I. Vasiliev, V. M. Kartak // System engineering and information technologies. - 2020. - V. 2, No. 2 (4). - S. 43-50.
7. Dovgal, V. A. Analysis of promising methods of behavioral biometrics for user authentication / V. A. Dovgal, D. V. Dovgal // Bulletin of the Adyghe State University. Series 4: Natural-mathematical and technical sciences. - 2017. - No. 3 (206). - S. 139-142.
8. Evsyukov, M. V., Putyato M. M., Makaryan A. S., Nemchinova V. O. Security methods in modern voice authentication systems // Caspian Journal: Management and High Technologies. - 2022. - No. 3 (59). - S. 84-92.
9. Litvin, I. I. Features of the collection, processing and protection of personal data by artificial intelligence / I. I. Litvin // Bulletin of the Ural Law Institute of the Ministry of Internal Affairs of Russia. - 2021. - No. 4. - S. 112-118.
10. Marshall, E. Security of artificial intelligence and machine learning: perspectives at Microsoft / E. Marshall, R. Rojas, D. Stokes, D. Brinkman // Microsoft. – 2022 [Electronic resource]. – Access Mode: https://learn.microsoft.com/en-us/security/engineering/securing-artificial-intelligence-machine-learning. – Access date: 11/15/2022.
11. Makhalina, O. M. Business digitalization increases the cost of information security / O. M. Makhalina, V. N. Makhalin // Management. - 2020. - No. 1. - S. 134-140.
12. Shabanov, A. Application of artificial intelligence technologies in information security / A. Shabanov // AM Live. – 2022 [Electronic resource]. – Access mode: https://www.anti-malware.ru/analytics/Technology_Analysis/using-artificial-intelligence-technologies-in-information-security. – Access date: 11/15/2022.
13. Moldamurat, K. Intelligent mechanism of hinding cryptographically protected communication channel / K. Moldamurat, D. Kalmanova, D. Yergaliyev, T. Beybithan // NiKa. – 2018. – no. 2. - S. 25-26.