Информационные технологии

УДК 004.056
DOI 10.34755/IROK.2023.96.12.189

КУЧЕРЯВЫЙ Е.А., д.т.н., доцент, главный научный сотрудник научной лаборатории, Научная лаборатория Интернета вещей и киберфизических систем, Московский институт электроники и математики им. А.Н. Тихонова НИУ ВШЭ, Департамент электронной инженерии.
Россия, Москва
Смирнов И.А. – аспирант, Московский институт электроники и математики им. А.Н. Тихонова НИУ ВШЭ, Департамент компьютерной инженерии, Методы и системы защиты информации, информационная безопасность.
РОССИЯ, МОСКВА

Анализ информационной безопасности на техническую спецификацию Network 2030 Architecture Framework для 6G сетей

Аннотация. В данной статье с точки зрения информационной безопасности (далее ИБ) рассматривается документ «FG NET-2030 Technical Specification on Network 2030 Architecture Framework» (далее ***Техническая спецификация***) выпущенный Международным союзом электросвязи (далее ITU) в 2020. Разработанная ***Техническая спецификация*** описывает архитектурные принципы для сетей общего пользования 6G, такие как: доступ, маршрутизация и адресация, безопасность сетевой передачи и другие аспекты.

На основании изученной ***Технической спецификации*** авторами статьи выявлены недостатки ИБ такие как: использование сетей общего пользования субъектами и не субъектами критической информационной инфраструктуры (далее КИИ); поддержка, унификация и интеграция старых протоколов; повышенная гетерогенность сети; отсутствие требований ИБ к Искусственному Интеллекту (далее ИИ или AI). Проанализировав данные недостатки, авторами статьи предложены решения, которые позволят избежать и митигировать выявленные риски ИБ для сетей общего пользования, критичной информационной инфраструктуры (далее КИИ) и искусственного интеллекта. Большинство решений ИБ в рассматриваемой ***Технической спецификации***, нуждаются в обновлении и доработке с точки зрения ИБ. При разработке и внедрении новой технологии нужно особое внимание уделять вопросам безопасности и защищенности самого решения, потому, что это позволит сохранить не только суверенитет, репутацию и материальные активы владельцев информации, но и предотвратить множество экономических, политических, социальных и других конфликтов и катастроф,

а также спасти жизни людей, что является приоритетной задачей информационной безопасности.

Ключевые слова: Network 2030, беспроводные технологии, сети 6G, техническая спецификация, информационная безопасность, риски, чувствительные данные, критическая информационная инфраструктура

Information security analysis on the Network 2030 Architecture Framework Technical Specification for 6G networks

Annotation. In this paper from the point of view of information security (hereinafter IS) the document "FG NET-2030 Technical Specification on Network 2030 Architecture Framework" (hereinafter Technical Specification) released by the International Telecommunication Union (hereinafter ITU) in 2020 is considered. The developed Technical Specification describes architectural principles for 6G public networks, such as: access, routing and addressing, security of network transmission and other aspects.

Based on the studied Technical Specification, the authors of the article have identified such IS drawbacks as: the use of public networks by subjects and non-subjects of critical information infrastructure (hereinafter referred to as CII); support, unification and integration of old protocols; increased network heterogeneity; lack of IS requirements for Artificial Intelligence (hereinafter referred to as AI). Having analyzed these shortcomings, the authors of the article propose solutions that will allow to avoid and mitigate the identified IS risks for public networks, critical information infrastructure (hereinafter referred to as CII) and artificial intelligence. Most of the IS solutions in the considered Technical Specification need to be updated and finalized from the IS point of view. When developing and implementing a new technology, it is necessary to pay special attention to the safety and security of the solution itself, because it will allow to preserve not only the sovereignty, reputation and material assets of information owners, but also to prevent many economic, political, social and other conflicts and disasters, as well as to save lives, which is a priority task of information security.

Keywords: Network 2030, wireless technologies, 6G networks, technical specification, information security, risks, sensitive data, critical information infrastructure.

1. Введение. Появление Интернета в 1980-х годах дало огромный толчок для развития человечества. С появлением спутников практически с любой точки планеты человек имеет возможность получить или отправить информацию через Интернет, используя телефон или лэптоп. Однако, далеко не вся передаваемая или получаемая информация является общедоступной. Среди информации ограниченного доступа выделяют государственную тайну, коммерческую тайну, тайну личной жизни, банковскую тайну, налоговую тайну, врачебную тайну, тайну усыновления, тайну связи, налоговую тайну,

нотариальную тайну, адвокатскую тайну, тайну страхования, служебную тайна, персональные данные, тайну голосования, тайну исповеди, и другие виды тайн.

Такие типы информации нуждается в защите согласно международному и локальному законодательству. Основываясь на требования законодательной и исполнительной власти, защита информации осуществляется с применением организационных и технических мер. Поэтому, при проектировании и разработке новой технологии, должны быть учтены эти особенности с перспективой ужесточения требований к ИБ, особенно, если данная технология обрабатывает чувствительные данные. Только в таком случае можно будет считать ту или иную разработку в перспективе безопасной, а обрабатывающуюся информацию в ней – достаточно защищенной. Как раз такие повышенные требования установлены и регламентированы государственными органами власти для систем банковской и гражданской инфраструктуры, тяжелой и легкой промышленности, энергетической и военной инфраструктуры, и к другим объектам КИИ. Напомним, что объект КИИ, согласно законодательству Российской Федерации — это информационные системы, отдельные узлы автоматизированного производства, а также телекоммуникационные системы и другие значимые системы [7].

Развитие и распространение систем искусственного интеллекта (далее AI) и Интернета вещей (далее IoT) в КИИ, а также в различные отрасли человеческой жизни (не относящиеся к КИИ), открывает новые горизонты развития науки и техники, что чрезвычайно важно для решения существующих вызовов, стоящих перед человечеством. Однако, данные системы требуют более совершенных и скоростных телекоммуникационных беспроводных технологий такие как 5G и 6G. Внедрение технологий 5G показали превосходные результаты скорости передачи информации 1 Гбит/с и задержку, которая составляет менее 30 миллисекунд, что на 23 миллисекунды быстрее, чем средние показатели 4G [8]. Но в 6G технологиях ожидается скорость передачи данных до 10 Тбит/с, а целевая задержка связи составляет от 1 секунды до 0.1 миллисекунды [9]. Внедрение 6G в ряде развитых стран планируется с 2030 года, а Южная Корея анонсировала запуск сетей класса 6G в 2028 году [10].

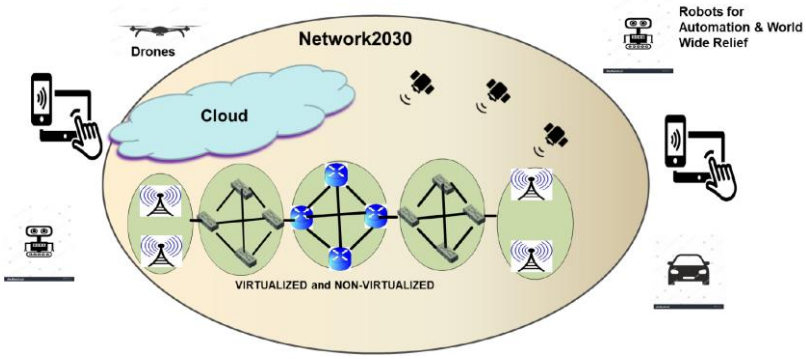

Рисунок 1 – Пример будущей сетевой инфраструктуры и конечных устройств [1]

В июне 2020 года ITU разработала техническую спецификацию [1] на сеть шестого поколения, которая, возможно, может стать Международным стандартом. Безусловно, данная ***Техническая спецификация*** будет неоднократно дорабатываться и пересматриваться ITU, но уже в ней можно отметить основные аспекты, на которые стоит обратить внимание со стороны ИБ, чтобы повысить уровень защищенности сети. В своем отчете [2] ITU отметили недостатки ИБ для сетей 6G такие как:

G.SEC.1. Пакетная авторизация,

G.SEC.2. Аутентификация заголовков пакетов и предотвращение спуфинга,

G.SEC.3. Гомоморфное шифрование

G.SEC.4. Безопасность услуг сети 2030: Скоординированные услуги

G.SEC.5. Безопасность услуг сети 2030: Качественные коммуникации

Несмотря на выявленный ITU перечень недостатков и проблем, которые нужно будет решить для 6G сетей, авторами данной статьи были выявлены еще ряд проблем, которые могут повлиять на ИБ в 6G.

Поэтому целью данной статьи является выявление недостатков и рисков ИБ в *Технической архитектуре* для сетей 6G, а также предложение вариантов их смягчения, основываясь на лучшие международные практики.

Риск 1 – Использование сетей общего пользования субъектами и не субъектами КИИ

Как известно, информационная безопасность определяется 4 основными принципами DICT (Доступность, Целостность, Конфиденциальность, Прослеживаемость). Придерживаясь этих принципов, сетевые технологии должны обеспечить в полной мере безопасность данных. В свою очередь, для каждой технологии определяется набор требований ИБ в зависимости от типа и назначения системы, а также обрабатываемых ею данных.

По словам авторов ***Технической спецификации***, сеть 6G будет предназначена «*для сетей общего пользования*»[4], однако по тексту самой архитектуры не раз упоминается использование данной технологии для взаимодействия с субъектами КИИ.

Если подходить с точки зрения ИБ, то архитектура сетей общего пользования должна отличаться от архитектуры сетей КИИ, т.к. нежелательно, чтобы в сетях общего пользования обрабатывалась чувствительная информация субъектов КИИ, которую злоумышленники смогут расшифровать, используя современные доквантовые и квантовые технологии. Напомним, что китайская компания Shenzhen SpinQ Technology в 2021 году предоставила промышленный двух кубитовый квантовый компьютер [3] для школ и учебных заведений, который можно было купить за пять тысяч долларов. Конечно, мощность этого квантового компьютера не сравнится с мощностью корпоративных квантовых компьютеров, способных обрабатывать более пятидесяти кубитов, но не стоит исключать вероятность того, что промышленные квантовые компьютеры к 2030 году будут обладать приблизительно такими же мощностями, как корпоративные квантовые компьютеры и будут доступны обычному потребителю, среди которых обязательно будут потенциальные киберпреступники.

Стоит отметить, что формулировка определения понятия КИИ [4] в большинстве стран мира разное, но имеют приблизительно одинаковые требования по защите. Поэтому, разрабатывая новую сетевую технологию, подход и требования к архитектуре объекта КИИ, как информационно-телекоммуникационные сети 6G, для взаимодействия с субъектами и не субъектами КИИ, должен быть разным, чтобы повысить уровень ИБ и защищенность данных. Добиться этого можно сегментированием сети и создать изолированные каналы обмена данными для групп участников сетевого взаимодействия, каждая из которых будет иметь собственную архитектуру и требования к ИБ. Предлагаем следующие категории групп:

- не субъекты КИИ,
- субъекты и не субъекты КИИ,
- субъекты КИИ.

Внедряя такой подход, можно будет контролировать потоки данных, что позволит уменьшить количество хакерских атак (например, D-DOS) на субъекты КИИ, значительно снизить случаи утечек чувствительных данных, повысить ИБ пользователей и участников сетевого взаимодействия.

Риск 2 – Поддержка, унификация и интеграция старых протоколов

В описании архитектурных принципов параграфа «8.2 Обратная совместимость» сказано: *«Сеть 2030 должна быть способна поддерживать, унифицировать и интегрировать протоколы, поддерживающие*

[4] ITU-T FG NET-2030 Technical Specification "Network 2030 Architecture Framework". Geneva, 2020, p.10

дифференциальные сервисы, которые оптимально удовлетворяют потребности новых микро (т.е. устройств IoT) и новых продвинутых устройств, вместе с существующими устройствами и обеспечивать такие возможности, как безопасность, конфиденциальность и детерминированная задержка.»[5].

Однако, авторы ***Технической спецификации*** не учитывают тот факт, что старые протоколы могут и будут содержать свои уязвимости, через которые можно воздействовать не только на данные, но и на оборудование. Приведем примеры.

Перед выходом данной ***Технической спецификации*** исследователи из Университета Пердью и Университета штата Айова (США) опубликовали статью [5] в 2019 году, в которой говорится, что ими был выявлен ряд новых уязвимостей в технологиях 4G и 5G, которые могут использоваться для перехвата звонков и отслеживания геопозиции пользователей. Чуть позже, в 2021 году, был опубликован доклад [6] согласно которому злоумышленники, используя эксплойты в алгоритмах GEA-1 и GEA-2 смогли расшифровать зашифрованный трафик более современного шифра, такого как GEA-3.

На основании вышеизложенного, существует риск того, что поддержка старых протоков и интерфейсов позволит злоумышленникам завладеть сетью.

Для смягчения описанного риска, авторы данной статьи предлагают ограничить использование старых протоколов в сетях 6G. А там, где это невозможно – необходимо использовать их модификации, которые будут соответствовать всем требованиям безопасности для взаимодействия с субъектами и не субъектами КИИ. Предложенное решение поможет значительно снизить вероятность взлома сети.

Риск 3 – Повышенная Гетерогенность сети

Гетерогенность (от греч. έτερος — другой + γένω — род) — разнородность, инородность; наличие неодинаковых частей в структуре, в составе чего-либо. Гетерогенные сети — сети, в которых присутствуют разные устройства не только с разными операционными системами, но и работающие по разным как технологиям, так и протоколам сети или разными реализациями этих протоколов. Разнородность в сетевых технологиях вызывает ряд проблемы со связью, например, обрывы соединения, потеря пакетов данных и ухудшение качества звука при звонке. Это происходит из-за того, что устройство переключается с одной базовой станции на другую, когда пользователь перемещается по зоне покрытия. Поэтому это является одной из ключевых проблем.

В ***Технической спецификации*** в параграфе «*Гетерогенность в коммуникациях, вычислениях, хранении, сервисах и их интеграции*» сказано, что «*в Сети 2030 гетерогенность будет гораздо выше и многомернее, чем*

[5] ITU-T FG NET-2030 Technical Specification "Network 2030 Architecture Framework". Geneva, 2020., p.26

сегодня. Будут существовать многочисленные типы сетевых устройств, сетевых и/или сервисных узлов, многочисленные протоколы, многочисленные сетевые и виртуальные сетевые функции, многочисленные услуги.»[6]. А с учетом того, что «*услуги Network 2030 не могут деградировать плавно*»[7], это может привести к деградации предоставляемых услуг таких как удаленная хирургия или тактильная связь, «*где увеличенная задержка может привести к потере иллюзии тактильного контроля, необходимого для уверенного управления удаленным оборудованием*»[8], степень гетерогенности сетей 6G необходимо снижать путем отказа от предыдущих технологий или их значительной модернизации, позволяющей уменьшить саму гетерогенность.

Если данную проблему рассматривать со стороны ИБ, увеличение гетерогенности в сетевых технологиях порождает множество проблем с обеспечением безопасности всех узлов сети, что приведет к усиленным требованиям безопасности использования 6G сетей, а, следовательно, к значительным затратам на услуги и технологии ИБ.

В связи с этим авторами данной статьи предлагается:

- максимально снизить неоднородность сети 6G, путем отказа от предыдущих технологий или их значительной модернизации, позволяющей уменьшить саму гетерогенность.

- внедрить процедуру и механизмы, позволяющие проверить настройки безопасности подключаемых устройств перед оказанием услуги Network 2030. В случае отсутствия требуемого уровня защищенности абонент будет перенаправлен оператором сети Network2030 на сети с предыдущем стандартом. Это решение позволит защитить не только данные, но и избежать мошенничества с чувствительными данными такими как персональные данные, генетические данные, биометрические данные, данные, касающиеся состояния здоровья, банковская тайна и пр.

Риск 4 – Отсутствие требований ИБ к Искусственному Интеллекту

Искусственный интеллект является очень сильным и продвинутым инструментом для решения большого количества задач разной сложности. Использование ИИ в работе позволяет не только автоматизировать любой процесс, но и настроить его в соответствии с конкретной задачей человека, ведомства или производства. Эффективность его применения доказана во многих областях таких как медицина, электронная коммерция, оборонное и военное дело, тяжелая и легкая промышленность, транспорт и логистика, системы информационной безопасности, космическая отрасль, спорт, образование, сельское хозяйство и животноводство, судебная система и т.д. Его использование позволило упростить и повысить качество выполняемых

[6] ITU-T FG NET-2030 Technical Specification "Network 2030 Architecture Framework". Geneva, 2020., p.26
[7] ITU-T FG NET-2030 Technical Specification "Network 2030 Architecture Framework". Geneva, 2020., p.41
[8] ITU-T FG NET-2030 Technical Specification "Network 2030 Architecture Framework". Geneva, 2020., p.41

задач, снизить нагрузку на человеческий ресурс и оптимизировать многие процессы. Поэтому логично было бы сделать обязательным применение ИИ в сетях нового поколения. Авторы ***Технической спецификации*** ожидают, что «*в Сети 2030 самоуправляемые сети и сервисы [ARCH.6] будут реализованы с использованием методов искусственного интеллекта и машинного обучения»*[9].

Таким образом, использование ИИ в сетях 6G поможет частично решить задачу отсутствие плавной деградации. Однако, авторы ***Технической спецификации*** не предъявляют требования к ИБ, которые должны применяться для систем ИИ, предоставляющих эти услуги. В самом программном коде внедряемого решения изначально могут быть заложены деструктивные программные закладки или быть уязвимости, которые могут повлиять не только на сам бизнес процесс, но и на безопасность всей сети. Особенно это может быть применимо для решений с открытым исходным кодом, таких как TensorFlow, PyTorch, Keras, Theano, Chat GPT и др. Поэтому крайне желательно, чтобы внедряемое ИИ решение прошло предварительную оценку со ИБ соответствующими организациями и было сертифицировано соответствующим надзорным органом для использования.

На текущий момент, в мировой практике существует множество документов, предъявляющих требования к безопасности ИИ, на основании которых можно будет в дальнейшем решить рассматриваемую проблему ИБ в ИИ. Вот некоторые из документов, которые предъявляют такие требования:

- Закон ЕС об ИИ (ARTIFICIAL INTELLIGENCE ACT) [11];
- "Временные меры по управлению генеративными службами искусственного интеллекта" [12], разработанные регуляторами КНР;
- Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года [13], утвержденная распоряжением Правительства Российской Федерации от 19 августа 2020 года N 2129-р;
- Ответственная стратегия искусственного интеллекта и пути ее внедрения [14], разработанная Пентагоном США в июне 2022 года.

Заключение

Развитие и внедрение 6G сетей способно решить существенное количество задач, которое ставится перед заинтересованными лицами. Особенно, если это связано с разработкой, развитием и внедрением новых технологий в современную жизнь, таких как ИИ и IoT, которые с максимальной эффективностью способны выполнять и оптимизировать сложнейшие задачи во всех сферах человеческой жизни. Использование квантовых технологий в беспроводных сетях нового поколения способно дать новые революционные решения в оптимизации и распределении ресурсов,

[9] ITU-T FG NET-2030 Technical Specification "Network 2030 Architecture Framework". Geneva, 2020., p.42

моделировании и прогнозирования, в криптографии и информационной безопасности.

Однако, не стоит пренебрегать мерами ИБ, т.к. любое воздействие на чувствительные данные пользователей или организаций, особенно относящихся к субъектам КИИ, может привести к серьёзным экологическим, экономическим, эпидемиологическим, военно-политическим и другим последствиям.

Найденные недостатки в ***Технической спецификации*** авторами данной статьи позволят в будущем повысить защищенность сетей шестого поколения, а предложенные решения позволят митигировать риски ИБ.

Поэтому, при разработке любого решения нужно большое внимание уделять вопросам ИБ. Ведь только тщательно продуманная архитектура разрабатываемого решения сможет выдержать любой удар, поможет избежать утечек данных и сохранить активы пользователей.

Литература

1. ITU-T FG NET-2030 Technical Specification "Network 2030 Architecture Framework". Geneva, 2020. URL: https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/Network_2030_Architecture-framework.pdf (дата обращения 06.06.2023)
2. ITU-T FG NET-2030 Technical Report "Gap Analysis of New Services, Capabilities and Use Cases for the Networks in 2030 and Beyond". Geneva, 2020. URL: https://www.itu.int/en/ITU-T/focusgroups/net2030/Documents/Gap_analysis_and_use_cases.pdf (дата обращения 12.07.2023)
3. A Desktop Quantum Computer for Just $5,000. A cheap, portable quantum computer, aimed at schools and colleges will be launched later this year. / DISCOVER [Электронный ресурс]. URL: https://www.discovermagazine.com/technology/a-desktop-quantum-computer-for-just-usd5-000 (дата обращения 07.07.2023)
4. Дремлюга Роман Игоревич КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА КАК ПРЕДМЕТ ПОСЯГАТЕЛЬСТВА В ЗАКОНОДАТЕЛЬСТВЕ ЗАРУБЕЖНЫХ СТРАН // Журнал зарубежного законодательства и сравнительного правоведения. 2022. №3. URL: https://cyberleninka.ru/article/n/kriticheskaya-informatsionnaya-infrastruktura-kak-predmet-posyagatelstva-v-zakonodatelstve-zarubezhnyh-stran (дата обращения: 19.09.2023).
5. Syed Rafiul Hussain (Purdue University), Mitziu Echeverria (University of Iowa), Omar Chowdhury (University of Iowa), Ninghui Li (Purdue University), Elisa Bertino (Purdue University). Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information. URL: https://s3.documentcloud.org/documents/5749002/4G-5G-paper-at-NDSS-2019.pdf (дата обращения: 19.09.2023)

6. Christof Beierle, Patrick Derbez , Gregor Leander , Gaetan Leurent , Havard Raddum , Yann Rotella , David Rupprecht , and Lukas Stennes. Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2. URL: https://eprint.iacr.org/2021/819.pdf (дата обращения: 19.09.2023)
7. Федеральный закон от 26.07.2017 N 187-ФЗ (ред. от 10.07.2023) "О безопасности критической информационной инфраструктуры Российской Федерации" / [Электронный ресурс] // Консультант Плюс : [сайт]. — URL: https://www.consultant.ru/document/cons_doc_LAW_220885/c5051782233acca771e9adb35b47d3fb82c9ff1c (дата обращения: 24.10.2023).
8. What is the Latency of 5G? / [Электронный ресурс] // News Center : [сайт]. — URL: https://www.verizon.com/about/our-company/5g/5g-latency (дата обращения: 24.10.2023).
9. Ученый ТУСУРа рассказал о развитии систем связи и технологии 6G на «Научной сессии ТУСУР» / [Электронный ресурс] // ТУСУР. TUSUR UNIVERSITY : [сайт]. — URL: https://tusur.ru/ru/novosti-i-meropriyatiya/novosti/prosmotr/-/novost-uchenyy-tusura-rasskazal-o-razvitii-sistem-svyazi-i-tehnologii-6g-na-nauchnoy-sessii-tusur (дата обращения: 24.10.2023).
10. S. Korea plans to launch 6G network service in 2028 / [Электронный ресурс] // Yonhap News Agency : [сайт]. — URL: https://en.yna.co.kr/view/AEN20230220003000320 (дата обращения: 24.10.2023).
11. ARTIFICIAL INTELLIGENCE ACT / [Электронный ресурс] // The AI ACT : [сайт]. — URL: https://artificialintelligenceact.eu/the-act/ (дата обращения: 24.10.2023).
12. Временные меры по управлению Генеративными службами искусственного интеллекта / [Электронный ресурс] // Офис Центральной комиссии по сетевой безопасности и информационным технологиям Государственное информационное бюро Китайской Народной Республики в Интернете : [сайт]. — URL: http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm (дата обращения: 24.10.2023).
13. ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ РАСПОРЯЖЕНИЕ от 19 августа 2020 N 2129-р Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года / [Электронный ресурс] // Электронный фонд правовых и нормативно- технических документов : [сайт]. — URL: https://docs.cntd.ru/document/565598768?marker=6560IO (дата обращения: 24.10.2023).
14. U.S. DEPARTMENT OF DEFENSE RESPONSIBLE ARTIFICIAL INTELLIGENCE STRATEGY AND IMPLEMENTATION PATHWAY / [Электронный ресурс] // D-Russia.ru : [сайт]. — URL: https://d-russia.ru/wp-content/uploads/2022/06/department-of-defense-responsible-artificial-intelligence-strategy-and-implementation-pathway.pdf (дата обращения: 24.10.2023).