Инженерный вестник Дона, №7 (2023)
ivdon.ru/ru/magazine/archive/n7y2023/8562

Эффективность шифрования данных в технологии беспроводного широкополосного доступа

Ш. М. Магомедгаджиев, Ф. С. Курбалиева

Дагестанский государственный университет

Аннотация: Статья посвящена обзору протоколов, используемых в широкополосных беспроводных сетях и методам защиты передачи информации в них с помощью алгоритмов шифрования. Рассмотрены теоретические и практические аспекты, особенности и принципы работы протоколов беспроводного доступа в сетях Wi-Fi, WiMax, GSM и др. Проведен обзор методов шифрования данных, используемых в них; уязвимости, встречающиеся в алгоритмах с пояснением и методами решения данных проблем, которые изучены в различных лабораториях. Целью исследования является обзор алгоритмов шифрования, используемых в протоколах беспроводного доступа. На основе проанализированных данных, сделан вывод об использовании алгоритмов AES и A5(128) и выявлены характерные для данных протоколов атаки и методы решения. Объектом исследования являются технологии беспроводного локального широкополосного доступа. Предмет исследования - алгоритмы шифрования, лежащие в основе беспроводных широкополосных сетей.
Научная новизна: проведен обзор уязвимостей в алгоритмах шифрования, применяемых в различных стандартах беспроводных сетей. Рассмотрены угрозы информационной безопасности, возникающие в стандартах шифрования AES и A5, относящиеся к атакам с использованием связанных и сеансовых ключей.
Ключевые слова: информационные технологии, криптография, защита данных, алгоритм шифрования, AES, A5, WiMax, Wi-Fi.

Введение

Важность широкополосной связи (BWA) признана во всем мире, данная технология обеспечивает высокоскоростной коммуникационный доступ с помощью беспроводных средств, для потребительского и делового рынка, способный удовлетворить растущий в условиях развития цифровой экономики спрос бизнеса на быстрое подключение к интернету и интегрированные услуги передачи данных в локальной сети. Широкополосный беспроводной доступ включает большое количество радиотехнологий и соответствующих услуг. С ее развитием становится актуальна проблема несанкционированного трафика при передаче информации по беспроводным каналам связи.

В данной работе подробно рассматривается текущее состояние протоколов, дается оценка их применения и перспектива исследования по защите информации.

Целью исследования является обзор эффективности шифрования данных в технологии беспроводного широкополосного доступа.

Для достижения цели были поставлены следующие задачи: провести обзор протоколов, используемых в беспроводных широкополосных сетях; рассмотреть используемые алгоритмы шифрования и методы обеспечения безопасности передачи данных.

Объектом исследования являются технологии беспроводного локального широкополосного доступа. «Широкополосный» означает предоставление различных видов услуг передачи данных с гарантированным качеством в одной и той же полосе пропускания системы. Корпоративные системы беспроводного широкополосного доступа предоставляют базовые услуги передачи данных, такие, как Интернет, VPN, VoIP, видеонаблюдение, видеоконференцсвязь, телевидение, передачу TDM-трафика, данных телеметрии.

Предметом исследования являются алгоритмы шифрования, лежащие в основе беспроводных широкополосных сетей и методы защиты, используемые при передаче информации.

Обзор

Вопрос о защите данных при передаче информации интересовал человечество всегда. Одним из первых известных способов защиты информации с помощью шифрования является шифр Цезаря [1]. С развитием информационных технологий менялись и методы передачи информации и шифрования. В настоящее время различные методы и средства защиту информации используют во всех информационных системах, проблема

является актуальной, однако этой теме посвящено недостаточно научных публикаций и специализированных изданий.

Проблеме передачи данных информации по широкополосным беспроводным сетям и перспективам применения в области организации защищенной связи посвящена диссертация и публикации Новикова С.Н., который рассматривает вопрос создания методологических основ и инструментов для обеспечения защиты информации на базе протоколов сетевого уровня и исследование методик и оценки угроз информационной безопасности [2-4]. Колыбельников А.И., в своих работах предлагает рассматривать проблему разработки методов и организации защиты данных беспроводных сетей с применением теории надежности [5, 6]. Проблема анализа эффективности применения шифрования в беспроводных сетях также рассматривается в научных работах Калашникова А.О., в которых он описывает модель сети с использованием механизма управления рисками [7, 8]. В работах Дворянкина С.В. исследованы особенности механизмов формирования уязвимостей мобильных устройствах [9, 10].

Результаты исследования и их обсуждение

Технологии широкополосного беспроводного доступа обеспечивают доступ к данным через беспроводную среду. Наиболее распространенным примером широкополосного беспроводного доступа является беспроводная локальная сеть. Экспоненциальный рост объемов трафика, связанных с развитием цифровых технологий, обуславливает необходимость приложения усилий по обеспечению повсеместной корректной работы беспроводных сетей путем разработки и развертывания передовых технологий радиодоступа, таких как 3GPP UMTS и LTE, а также мобильных систем WiMAX [11].

Фиксированный BWA предоставляет услуги беспроводного интернета для устройств, расположенных в более или менее ограниченных местах,

таких, как дома и офисы. Услуги сравнимы с услугами, предоставляемыми через цифровую абонентскую линию (DSL) или кабельный модем, с тем отличием, что он имеет беспроводной режим передачи.

Существуют две основные технологии, используемые в фиксированном BWA:

• LMDS (локальная многоточечная система распределения);

• Системы MMDS (многоканальная многоточечная служба распределения).

Мобильный BWA, также называемый мобильным широкополосным доступом, обеспечивает высокоскоростное широкополосное соединение от поставщиков услуг мобильной связи, которое доступно из случайных мест. Однако данные системы в основном ориентированы на фиксированные широкополосные сети и требуют использования устройств, которые подключаются к кабельным или DSL-модемам для измерения скорости и качества домашних интернет-соединений [12].

Wi-Fi (Wireless Fidelity), использует радиоволны для обеспечения беспроводного высокоскоростного доступа в интернет и сетевых подключений. Обнаружение сетей Wi-Fi, к которым подключался пользователь, может быть использовано для установки поддельных точек доступа и проведения атак «Человек посередине», что потенциально может считывать сетевой трафик пользовательского устройства. Сенсорная сеть может быть развернута для мониторинга канала WiFi для этого конкретного трафика MAC, таким образом, отслеживая местонахождение пользователя [13].

Основными уровнями модели OSI для беспроводных широкополосных технологий доступа являются:

Физический уровень отвечает за кодирование и декодирование сигналов и управляет передачей и приемом битов. Он преобразует кадры

уровня MAC в сигналы для передачи. Схемы модуляции, которые используются на этом уровне, включают в себя: QPSK, QAM-16 и QAM-64.

Уровень MAC (канальный) обеспечивает интерфейс между уровнем конвергенции и физическим уровнем стека протоколов WiMax и Wi-Fi. Он обеспечивает многоточечную связь и основан на CSMA/CA (множественный доступ с контролем несущей и предотвращением конфликтов).

Уровень конвергенции (сетевой) предоставляет информацию о внешней сети. Он принимает блок данных протокола более высокого уровня (PDU) и преобразует его в PDU более низкого уровня, а также предоставляет функции в зависимости от используемой службы.

WiMAX расшифровывается, как Wireless Inter-operability for Microwave Access (широкополосная связь на значительные расстояния). Эта технология используется для обеспечения более высоких скоростей передачи данных с увеличенным покрытием, основана на стандарте IEEE 802.16 и технологии MAN (Metropolitan Area Network). WiMAX использует лицензированный или нелицензированный спектр для подключения к сети, работает с более крупной интероперабельной сетью, также ее можно использовать для предоставления интернет-услуг, таких, как мобильные данные и точки Wi-Fi. В настоящее время поставщиками сертифицированных устройств с поддержкой технологии WiMAX являются более ста компании со всего мира: Intel, Alcatel, Siemens, AT&T, WiLAN и др., а также известные на российском рынке компании Asiros, Airspan, Alvarion, Aperto, Proxim и Wi-LAN.

Сверхширокополосный (UWB) — это протокол, подобно Bluetooth и Wi-Fi, беспроводной связи малого радиуса действия, работающий посредством радиоволн. Но, в отличие от своих аналогов, он работает на очень высоких частотах — в широком спектре частот в гигагерцах — и

может использоваться для сбора высокоточных пространственных и направленных данных.

Глобальная система мобильной связи (GSM) в настоящее время является наиболее часто используемым методом связи, поскольку она обеспечивает наилучшие сетевые возможности и возможности глобального роуминга. Таким образом, реализации удаленных систем на основе GSM являются надежными методами и используются во многих приложениях по всему миру. Это программа широкомасштабных коммуникационных технологий, которая использует цифровые радиоканалы для создания аудио, информационных и мультимедийных систем связи.

В нашем исследовании проблема защиты беспроводных сетей рассматривалась в аспекте использования алгоритмов шифрования в протоколах Wi-Fi, WiMax, UWB, GSM.

В таблице 1 приведены основные технологии беспроводных сетей, применяемые алгоритмы шифрования и наиболее распространенные угрозы информационной безопасности.

Алгоритм шифрования AES (Advanced Encryption Standard) основан на сети замещения-перестановки, также известной, как сеть SP, состоит из ряда связанных операций, включая замену входных данных конкретными выходными данными (подстановки) и перетасовку битов (перестановки).

Беспроводные сети имеют встроенное программное обеспечение и полные системы безопасности, основанные на этом алгоритме, и теперь они используются в повседневной жизни. Несмотря на то, что AES является исключительно безопасным типом шифрования, до сих пор не было зарегистрировано ни одного известного успешного реального нападения. Тем не менее, ни одна система шифрования не является полностью безопасной. Исследователи, изучавшие AES, протестировали некоторые виды атак.

В 2018 году была обнаружена возможная атака с использованием связанных ключей [14].

Таблица № 1

Алгоритмы шифрования и их возможные уязвимости

№	Наименование технологии	Алгоритм шифрования	Режим	Возможные атаки
1	Персональные (Bluetooth, ZigBee, Insteo ZigBeen, Z-Wave)	E0, AES, Rolling code system, 3DES	ECB, CBC, Поточное, ECB	Атака на ключ шифра AES, Атаки по побочным каналам, «Биклик», Атака на основе коллизий, Атака линейным анализом, Атака дифференциальным анализом.
2	Локальные (WI-FI, UWB, RuBee)	RC4, AES	CBC	Атака Флюрера, Мантина и Шамира, Атака на ключ шифра AES, Атака на основе коллизий, Атака начального заполнения R4.
3	Городского масштаба (WIMAX)	3DES, AES	ECB	Атака на ключ шифра AES, Атака на основе коллизий, Атака линейным анализом, Атака дифференциальным анализом.
4	Глобальные (GSM, UMTS, GPRS, PDC, IDEN, CDMA)	A5 (COMP-128), GEA1, GEA2, CMEA	Поточное, CBC	Атака Андерсона, Атака методом вскрытия A5, Атака прямого перебора.

В отличие от атак «грубой силы», которые можно использовать в алгоритме DES, атаки с использованием связанных ключей нацелены на сам ключ шифрования. Они требуют меньше времени и усилий и имеют больше

шансов на успех. Этот тип атаки может быть реализован, если злоумышленник знает (или подозревает) взаимосвязь между двумя разными ключами.

В том же году была попытка взломать AES-128 с помощью атаки с распознаванием известного ключа [14]. Она оказалась успешной, против 8-раундовой версии шифрования AES с длиной 128-битного ключа. Однако настоящий AES-128 проходит 10 раундов шифрования, а это значит, что в реальной жизни атака не представляла угрозы.

Несколько раз шифрование AES становилось целью атак с использованием связанных ключей. Чтобы предотвратить подобные виды атак, криптографы усложнили расписание ключей AES. Применение алгоритма шифрования AES показано на рис.1.

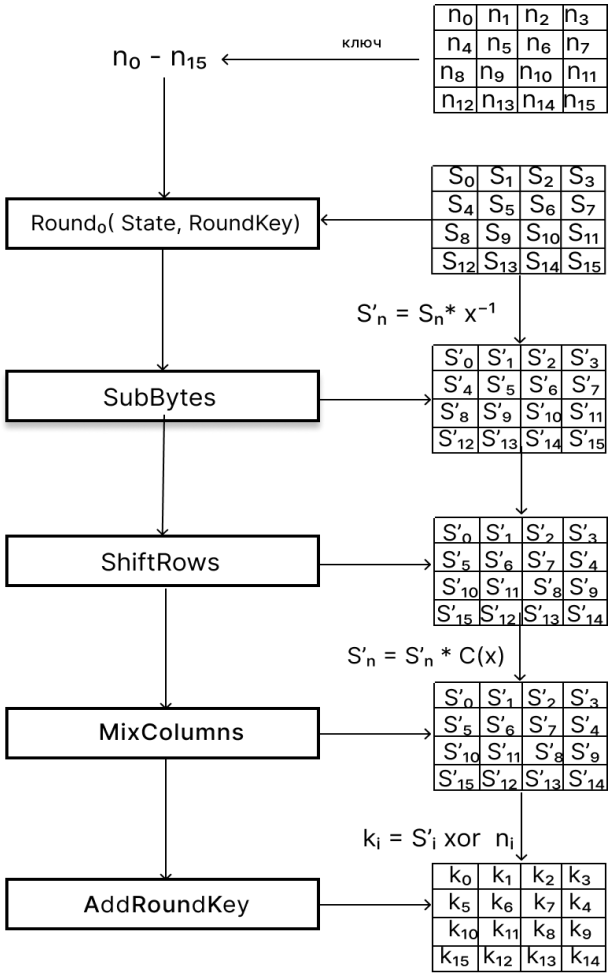

Рис. 1. – Схема работы алгоритма AES

Один раунд AES состоит из 3 слоев: линейного слоя смешения (диффузии), нелинейного слоя и слоя добавления ключей. Эти 3 уровня выполняются следующими 4 функциями: SubByte, ShiftRow, MixColumn, AddRoundKey.

Алгоритм AES работает с массивом размерностью 4×4.

На шаге SubBytes каждый байт заменяется его записью в фиксированной 8-битной таблице поиска.

На шаге ShiftRows байты в каждой строке состояния циклически сдвигаются влево. Количество мест, на которые сдвигается каждый байт, постепенно различается для каждой строки.

На шаге MixColumns каждый столбец состояния умножается на фиксированный полином. На последнем шаге AddRoundKey каждый байт состояния объединяется с байтом раундового подключа с помощью операции XOR (⊕) [15].

Отличительные атаки с известным ключом

Исследователи швейцарской ИТ-компании Terra Quantum AG с помощью квантового компьютера обнаружили уязвимости, которые влияют на симметричные шифровальные шифры, в том числе, AES, который широко используется для защиты данных, передаваемых через Интернет. Используя метод, известный как квантовый отжиг, компания заявила, что ее исследование показало, что даже самые надежные версии шифрования AES могут быть расшифрованы квантовыми компьютерами, которые могут быть доступны через несколько лет [16]. Предположительно, данные проблемы ставят под угрозу конфиденциальность данных в сети и транзакций и электронной почты.

Алгоритм A5 — это поточный алгоритм шифрования, используемый для обеспечения конфиденциальности передаваемых данных между телефоном и базовой станцией в европейской системе мобильной цифровой

связи GSM. Потоковое шифрование инициализируется сеансовым ключом и номером расшифровываемого/дешифруемого кадра. Один и тот же сеансовый ключ используется на протяжении всего вызова, но 22-битный номер кадра меняется во время вызова, таким образом генерируя уникальный ключевой поток для каждого кадра.

Генератор A5 состоит из трех регистров сдвига с линейной обратной связью – РСЛОС, длиной 19, 22 и 23 разряда, соответственно (в сумме 64 разряда), заданных следующими полиномами обратной связи (рис. 2.).

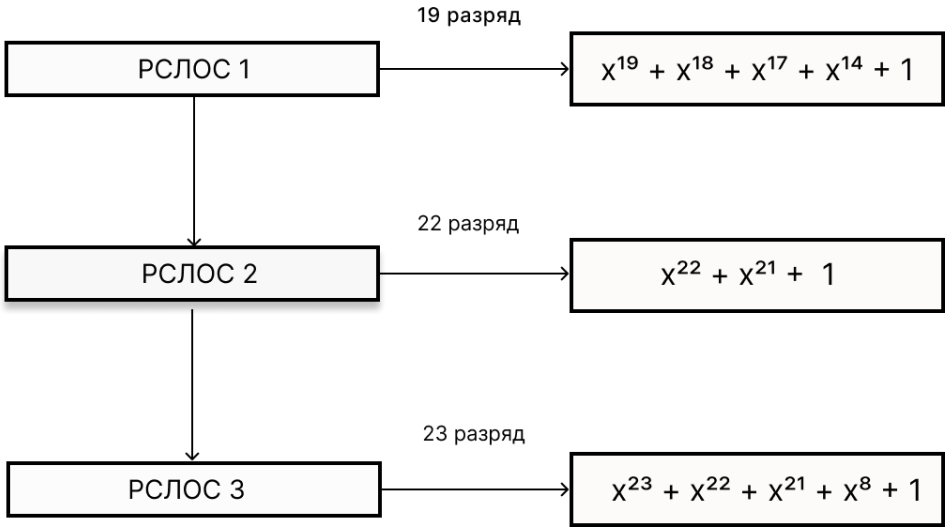

Рис. 2. – Схема работы алгоритма A5

В начале каждого такта РСЛОС значения самых старших бит регистров складываются операцией XOR. Полученное таким образом значение становится следующим битом ключевого потока. РСЛОС в A5 сдвигаются несинхронно, а с помощью равенства (1).

$$b_1^t = maj\left(b_1^t, b_2^t, b_3^t\right), \quad (1)$$

где maj –булева функция большинства, b_i – средний разряд регистра.

Вопрос о модели безопасности GSM заключается в том, можно ли прослушивать вызов, когда по крайней мере один из алгоритмов, от которых он зависит, оказался неисправным. Большинство ученых во всем мире единодушны в том, что перехват по воздуху и декодирование вызова в

реальном времени по-прежнему невозможно, несмотря на уменьшенное пространство ключей. Но, есть и другие способы атаки на систему, которые осуществимы и являются вполне реальными угрозами. Есть также много реалистичных атак, которые не связаны с ошибками в алгоритмах безопасности.

Атака по принципу «разделяй и властвуй» основана на атаке с известным открытым текстом. Злоумышленник пытается определить начальные состояния LSFR по известной последовательности потока ключей. Злоумышленнику необходимо знать 64 последовательных бита ключевого потока, которые можно получить, если злоумышленник знает некоторый зашифрованный текст и соответствующий открытый текст. Это во многом зависит от формата кадров GSM, отправляемых туда и обратно. Кадры GSM содержат много постоянной информации, например, заголовки фреймов. Требуемые 64 бита не всегда могут быть известны, но обычно известно от 32 до 48 бит, иногда даже больше.

Решением данной уязвимости послужило использование новой реализации A5 с сильным шифрованием (128), чтобы атака грубой силы была невозможна в любом случае. Это лишило бы злоумышленника возможности записывать передаваемые кадры и взламывать их в свободное время. Это усовершенствование потребует сотрудничества с Консорциумом GSM. Эти уязвимости потенциально могут раскрыть личные SMS-сообщения, личные данные и даже местоположения GPS для общественности, если их не защитить. Необходимы дополнительные исследования в этой области, чтобы обеспечить безопасность нашей конфиденциальности. С точки зрения информационной безопасности, проблемными областями могут быть атаки MiTM и взломы сети.

Вывод

В настоящее время функционирует достаточно большое количество сетей беспроводного доступа, специфика которых не может обеспечить высокий уровень защиты информации, например, глобальные сети, которые являются неустойчивыми к атакам на алгоритмы шифрования.

В статье проанализированы особенности беспроводных широкополосных технологий доступа и применяемых в них алгоритмов шифрования, рассмотренные беспроводные сети, в соответствии с протоколами шифрования и потенциальными атаками, встречающимися в данных технологиях.

Анализ различных исследований, связанных с возможными атаками и выявлением уязвимостей в протоколах беспроводного доступа, показал, что наиболее защищенными и широко распространенными являются сети, использующие алгоритмы шифрования AES и 3DES, этот вывод подтверждается и при исследовании устойчивости алгоритмов к квантовым вычислениям.

Литература

1. Гумерова Л.З., Аглямзянова Г.Н., Маисеева Е.С. Взлом шифра Цезаря методом «грубой силы» // Лучшие практики общего и дополнительного образования по естественно-научным и техническим дисциплинам: материалы II Всероссийской научно-практической конференции, посвященной памяти академика РАН К.А. Валиева. Казань, 2022. С. 157-163.

2. Новиков С.Н. Методология защиты информации на основе технологий сетевого уровня мультисервисных сетей связи: дис. … д-р. тех. наук. – Томск.: ТУСУР, 2016. – С. 235.

3. Смирнов Р.А., Новикова А.С., Новиков С.Н. Анализ методик оценки безопасности информации в телекоммуникационных системах //

Современные проблемы телекоммуникаций: материалы Российской научно-технической конференции. Новосибирск. 2022. С. 218-221.

4. Смирнов Р.А., Новиков С.Н. Исследование методик оценки угроз безопасности информации // Интерэкспо Гео-Сибирь. 2022. Том 6. С. 250-257.

5. Колыбельников, А. И. Обзор технологий беспроводных сетей // Труды МФТИ. - 2012. Том 4, № 2. С.3-29.

6. Kolybelnikov A.I. Trust model, reliability theory in theory of secrecy. 2021 international conference engineering and telecommunication, En and T 2021. pp. 1-4.

7. Калашников А.О., Аникина Е.В. Управление рисками сложной сети на основе обобщенной арбитражной схемы // Вопросы кибербезопасности. 2022. № 1(47). С.95-101.

8. Калашников А.О., Щербаков В.Б., Борисова М.Г., Резов А.А., Ермаков С.А. Оценка и регулирование рисков атакуемых беспроводных сетей при блокировании их элементов // Информация и безопасность. 2017. № 2. С. 155-184.

9. Михайлов Д.М., Дворянкин С.В., Чуманская В.В. Подходы к математическому моделированию кибератак на мобильные устройства // Вопросы кибербезопасности. 2021. №6(46). С. 62-67.

10. Дворянкин С.В., Дворянкин Н.С. Речеподобные сигналы для защиты речевой информации в каналах голосовой связи // Информационная безопасность: вчера, сегодня, завтра: Сборник статей по материалам III Международной научно-практической конференции. Москва. 2020. С. 78-85.

11. Swain C.M.K., Das S. Proposed prediction framework for improving the accuracy of path loss models of WiMax network // Wireless personal communications. 2021. № 117(4), pp. 1-23.

12. Suraci C., Araniti G., Abrardo A., Bianchi G., Iera A. A stakeholder-oriented security analysis in virtualized 5G cellular networks // Computer networks. 2020. № 184 URL: researchgate.net/publication/345314523 _A_Stakeholder-Oriented_Security_Analysis_in_Virtualized_5G_Cellular_ Networks .

13. Килин А. С. Обнаружение сигнатур атак в WiFi-сети методами машинного обучения // Студент и научно-технический прогресс: Сборник трудов XIII научной конференции молодых ученых. Челябинск. 2019. С. 405-408.

14. Уривский А.В. Принципы проектирования сетевых протоколов распределения ключей для квантовых сетей // Труды МФТИ. 2022. Том 14. №2(54). С.136-148.

15. Архипова И.С Криптографический алгоритм AES как средство защиты информации // Аллея науки. 2018. Том 6. № 4(20). С. 83-87.

16. A Swiss Company Says It Found Weakness That Imperils Encryption / URL: terraquantum.swiss/news/a-swiss-company-says-it-found-weakness-that-imperils-encryption.

References

1. Gumerova L.Z, Aglyamzyanova G.N, Maiseeva E.S. Luchshie praktiki obshhego i dopolnitel`nogo obrazovaniya po estestvenno-nauchny`m i texnicheskim disciplinam: materialy` II Vserossijskoj nauchno-prakticheskoj konferencii, posvyashhennoj pamyati akademika RAN K.A. Valieva. Kazan. 2022. pp. 157-163.

2. Novikov S.N. Metodologiya zashhity` informacii na osnove texnologij setevogo urovnya mul`tiservisny`x setej svyazi [Methodology of information protection based on network technologies of multiservice communication networks]: dis. … DEng. Tomsk: TUSUR. 2016. pp. 235.

3. Smirnov R.A., Novikova A.C., Novikov S.N. Sovremenny`e problemy` telekommunikacij: materialy` Rossijskoj nauchno-texnicheskoj konferencii. Novosibirsk. 2022, pp. 218-221.

4. Smirnov R.A., Novikov S.N. Intere`kspo Geo-Sibir. 2022. Volume 6. pp. 250-257.

5. Kolybelnikov A.I. Trudy MFTI [Works MIPT]. 2012. Volume 4, №. 2. pp. 3-29.

6. Kolybelnikov A.I. Trust model, reliability theory in theory of secrecy. 2021 international conference engineering and telecommunication, En and T 2021. 2021. pp. 1-4.

7. Kalashnikov A.O., Anikina E.V. Voprosy` kiberbezopasnosti. 2022. № 1(47). pp. 95-101.

8. Kalashnikov A.O., Shcherbakov V.B., Borisova M.G., Rezov A.A., Ermakov S.A. Informaciya i bezopasnost. 2017. № 2. pp. 155-184.

9. Mikhailov D.M., Dvoryankin S.V., Chumanskaya V.V. Voprosy` kiberbezopasnost. 2021. № 6(46). pp. 62-67.

10. Dvoryankin S.V., Dvoryankin N.S. Informacionnaya bezopasnost`: vchera, segodnya, zavtra: Sbornik statej po materialam III Mezhdunarodnoj nauchno-prakticheskoj konferencii. Moskva. 2020. pp. 78-85.

11. Swain C.M.K., Das S. Wireless personal communications. 2021. № 117(4). pp. 1-23.

12. Suraci C., Araniti G., Abrardo A., Bianchi G., Iera A. Computer networks. 2020. № 184 URL: researchgate.net/publication/345314523 _A_Stakeholder-Oriented_Security_Analysis_in_Virtualized_5G_Cellular_ Networks .

13. Kilin A.S. Student i nauchno-texnicheskij progress: Sbornik trudov XIII nauchnoj konferencii molody`x ucheny`x. Chelyabinsk. 2019. pp. 405-408.

14. Urivsky A.V. Trudy MFTI [Works MIPT]. 2022. Volume 14. №2 (54). pp.136-148.

15. Arkhipova I.S. Alleya nauki. 2018. Volume 6. № 4(20). pp. 83-87.

16. A Swiss Company Says It Found Weakness That Imperils Encryption, URL: terraquantum.swiss/news/a-swiss-company-says-it-found-weakness-that-imperils-encryption.