АНАЛИЗ НЕКРИПТОГРАФИЧЕСКИХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В РАДИОКАНАЛАХ ИНФОРМАЦИОННЫХ СИСТЕМ

Махов Д. С.[1],

DOI: 10.21681/2311-3456-2024-1-82-88

Цель исследования *состоит в анализе проблемных вопросов определения понятия некриптографических методов, показателей и критериев защиты информации в радиоканале, а также в кратком анализе существующих методов борьбы с помехами и возможности их использования в качестве некриптографических методов защиты информации в радиоканале.*

Методы исследования: *в работе применен дедуктивный подход к определению понятия «защита информации в радиоканале». Затем на основе логического вывода и индуктивного подхода проведено соотнесение показателей защищенности информации и показателей, применяемых для оценки радиотехнических систем при воздействии помех.*

Результат исследования: *на основе сочетания метода аналогии и дедуктивного подхода установлены взаимосвязи между показателями защиты информации и показателями оценки радиотехнических систем при воздействии помех. Изложен проблемный вопрос о нормативном определении понятия «некриптографических» методов защиты информации в радиоканале. На основе анализа научных публикаций по теме исследования приведено краткое описание методов борьбы с помехами и их влияния на защищенность радиотехнической системы, как информационной. Предложено в качестве математического аппарата оценивания использовать аппарат теории вероятностей. Намечены пути установления аналитической взаимосвязи показателей защищенности информации в радиоканале и параметров радиотехнических систем.*

Практическая ценность: *предложен подход к аналитическому описанию защищенности информации в радиоканалах. Это позволит учитывать показатели как криптографических, так и некриптографических методов защиты информации при анализе защищенности информационных систем. Определено направление научных исследований, которое позволит дать нормативное определение и сформировать классификацию некриптографических методов защиты информации в радиоканалах, что может быть использовано при синтезе систем и средств защиты информации.*

Ключевые слова: *оценочно-критериальная база, радиотехническая система, защищенность информации, конфиденциальность, доступность, помехоустойчивость, скрытность, воздействие помех, пространственная селекция, фильтрация, расширение спектра.*

ANALYSIS OF NON-CRYPTOGRAPHIC INFORMATION PROTECTION METHODS IN WIRELESS INFORMATION SYSTEMS

Makhov D.S.[2]

The purpose *of the research is to analyze the problematic issues of the non-cryptographic methods concept defining, indicators and criteria for information protection in the radio channel, as well as an existing interference resistance methods analysis, and the using possibility of their as non-cryptographic information secure methods in the radio channel.*

1 Махов Денис Сергеевич, доктор технических наук, начальник кафедры защиты информации в радиолиниях систем и комплексов вооружения, военной и специальной техники Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С. М. Штеменко, г. Краснодар, Россия. E-mail: sinedvoham@yandex.ru

2 Denis S. Makhov, Dr.Sc. (in Engineering sciences), Head of department information secure in radio channel of the military equipment systems Krasnodar Higher Military Orders of Zhukov and the October Revolution of the Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: sinedvoham@yandex.ru

Research methods: *the article uses a deductive approach to the definition of the «radio channel information secure» concept. Then, on the logical inference basis and an inductive approach, the correlation of information security indicators and radio engineering systems evaluation indicators under the interference influence was carried out.*

The research result: *on the analogy method and the deductive approach combination basis, the interrelationships between information security indicators and radio engineering systems evaluation indicators under the interference influence have been established. The normative definition problem of the information security «non-cryptographic» methods concept in the radio channel is presented. Based on the research field scientific publications review, the interference resistance methods description and their influence on the security of the radio engineering system as an information system is given. It is proposed to use the probability theory methods as a mathematical evaluation instrument. The ways of establishing an analytical relationship between the information security indicators in the radio channel and the radio engineering systems parameters are defined.*

Practical significance: *an approach to the information security analytical description in radio channels is proposed. This way allows taking into account the indicators of both cryptographic and non-cryptographic information protection methods during the information systems security analyze. The scientific research direction to give a normative definition and form a non-cryptographic information security methods classification in radio channels has been determined. This can be used in the information security systems and tools synthesis.*

Keywords: *evaluation and criteria base, radio engineering system, information security, confidentiality, accessibility, interference immunity, stealth, interference influence, space selection, filtering, spectrum spreading.*

Введение

В настоящее время увеличивается количество информационных систем как гражданского, так и военного назначения, осуществляющих информационный обмен по радиоканалам (РК), вследствие чего возникает множество проблем обеспечения информационной безопасности таких систем [1, 2]. Это повышает актуальность вопроса защиты всех видов информации, передаваемой по РК, от воздействий внешних и внутренних вредных факторов. Нормативными документами предписано делить методы защиты информации в РК на криптографические и некриптографические. И если криптографические методы защиты информации в РК определены и известны [3], то понятие некриптографических методов для области защиты информации в РК не определено. Возникают проблемные вопросы определения понятия «некриптографические методы», классификации самих методов в области защиты информации в РК, решения практических задач на их основе. Существует некоторое количество публикаций, сводящих вопросы защиты информации в РК не криптографическими методами к области технической защиты от побочных электромагнитных излучений [4] или к вопросам защиты от несанкционированного доступа [5].

Как правило, показатели и критерии оценивания защищенности информации в РК в данных публикациях весьма расплывчаты, что затрудняет формирования критической оценки преимущества тех или иных «некриптографических» методов[3] [6]. Следует отметить, что в случае, когда средой распространения информации между двумя элементами информационной системы является воздушное пространство, то такая система коренным образом отличается от других типов систем не только по оценочно-критериальной базе ее функций, но и по инструментарию обеспечения ее эффективного функционирования [7]. Это связано с тем, что основным внешним вредным фактором для такой системы являются электромагнитные помехи на основе известного факта, что в свободном пространстве информация переносится с помощью электромагнитных волн. Как известно [8, 9], воздействие помех на функционирование информационной системы в РК осуществляется, как правило, в свободном пространстве на сигнальном, или, согласно понятийному аппарату информационных систем, на физическом уровне эталонной модели взаимодействия открытых систем (ЭМВОС).

Следует также упомянуть, что информационные системы, информация в которых циркулирует по РК, называются радиотехническими системами (РТС). Оценке эффективности функционирования РТС посвящено достаточное количество литературы, отражающей более ста лет накопленных знаний в области радиотехники. Определены показатели, критерии оценки, стандарты и рекомендации, разработаны методы достижения значений показателей, определены оптимальные значения (например, порог Шеннона) а также пути научного развития. Вместе с тем, анализ показал, что такие показатели для вопросов защиты информации в РТС отсутствуют, а показатели криптографических методов не учитывают особенности функционирования РТС.

3 Брауде-Золотарев Ю.М. Алгоритмы безопасности радиоканалов // Алгоритм безопасности. 2013. № 1. С. 64–66.

На основании вышеизложенного возникает противоречие, заключающееся в том, что с одной стороны в РТС строго определены информационные показатели для криптографических методов защиты информации в РК, которые не учитывают влияние внешних вредных факторов физического и канального уровней ЭМВОС, а с другой стороны внешние вредные факторы учитываются в радиотехнических показателях оценки РТС, но не определены для информационных показателей некриптографических методов защиты информации в РК.

Анализ оценочно-критериальной базы защиты информации в радиоканалах

Для разрешения указанного противоречия необходим анализ понятий и определений из области защиты информации, которые служат или могут служить показателями оценки систем передачи информации в РК.

Как известно объектом защиты информации являются носители информации, под которыми понимается в том числе физическое поле, отражающее информацию в виде символов, образов и сигналов[4].

На основе этого тривиален вывод, что любая система связи есть система передачи информации. Это также подтверждается документально. В частности, из нормативных документов следует, что радиосвязь – электросвязь, осуществляемая посредством радиоволн[5]. А в нормативном документе по электросвязи приводится определение электросвязи[6], такое что «Электросвязь – это любые излучения, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам». При этом, как известно, информационная система – это система, в том числе обрабатывающая и выдающая информацию для дальнейшего использования. Отсюда следует, что РТС является информационной системой. В РТС информация отражена битовым потоком, в двустороннем порядке модулирующим несущие колебания, преобразуемые в дальнейшем в электромагнитные волны. Так что все информационные показатели имеют место и могут преломляться для РТС, в том числе касаемо функций и методов защиты информации в РК.

Таким образом, связь – есть передача информации за исключением случаев, когда канал связи имеется, а информация по нему не передается.

Теперь рассмотрим понятия области защиты информации касательно методов защиты информации в РК. В нормативных документах по защите информации указано, что защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных (но преднамеренных) и непреднамеренных воздействий на нее.

Для обеспечения безопасности информации, под которой можно понимать конечный результат, достижение цели защиты, перевод информационной системы (РТС) в состояние защищенности, используются два типа защиты – техническая и криптографическая. Также существует определение криптографической защиты информации, как ЗИ с помощью ее криптографического преобразования.

При этом в определении технической защиты информации фигурирует понятие некриптографических методов. А именно, под технической защитой информации, как ЗИ заключающейся в обеспечении некриптографическими методами безопасности информации, подлежащей защите с применением технических, программных и программно-аппаратных средств. Но вместе с тем определение некриптографических методов, как всех, которые не подпадают под определение криптографических, весьма расплывчато и не определено (рис. 1).

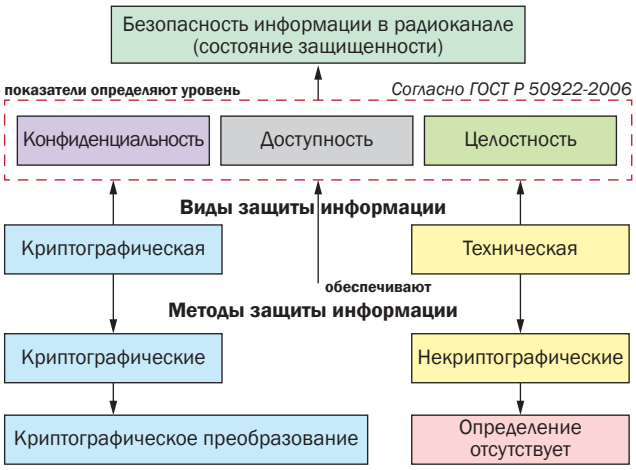

Рис.1. К определениям методов защиты информации, отраженных в нормативных документах

На основе вышеизложенного к некриптографическим можно отнести традиционные и вновь создаваемые методы повышения уровня таких показателей, как помехозащищенность, помехоустойчивость и скрытность [10]. Однако возникает неопределенность оценивания эффективности таких методов с точки зрения защиты информации, обусловленная отсутствием теоретического базиса и аналитического описания показателей защиты информации в РК для РТС.

В силу того, что показатели защиты информации имеют лишь нормативное определение, возможна попытка их аналитического описания с помощью вероятностного подхода. Обозначая использование

4 ГОСТ Р 50922–2006. Защита информации. Термины и определения. – М.: Стандартинформ, 2008. – 12с.

5 ГОСТ 24375-80. Радиосвязь. Термины и определения. – М.: Издательство стандартов, 1987. – 57 с.

6 ГОСТ Р 53111-2008. Устойчивость функционирования сети электросвязи. Требования и методы проверки. – М.: Стандартинформ, 2011. – 31 с.

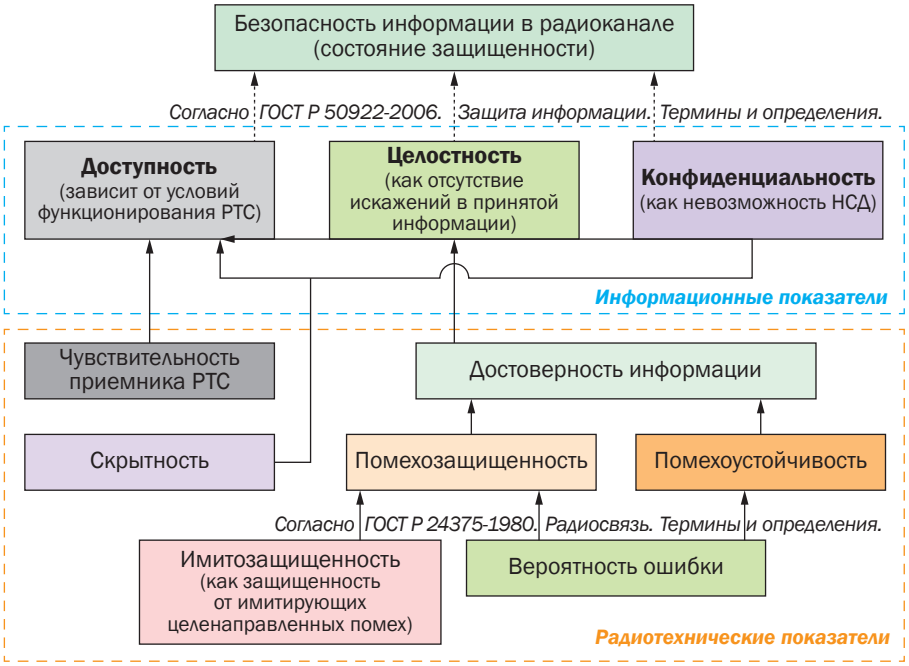

Рис.2. Вариант установления связей между показателями, характеризующими свойства информации в РК и показателями, характеризующими РТС

для защиты РК криптографических методов в виде M, а некриптографических – N, функцию, описывающая состояние защищенности информации можно представить в следующем виде:

$$Z = \rho(M) + \rho(N) - \rho(MN), \quad (1)$$

где: ρ – вероятность.

Описание в виде (1) может правомерно служить основой для расчета защищенности информации в РК. Однако для установления связи между параметрами РТС и показателями защищенности информации необходимо рассмотреть основные показатели защиты информации (рис. 2).

Состояние защищенности информации, ее безопасность, обеспечивается ее конфиденциальностью C, доступностью D и целостностью S и является их функцией2:

$$Z = f(D,C,S). \quad (2)$$

Конфиденциальность – обязательное для выполнения лицом, получившим доступ к информации требование не передавать такую информацию третьим лицам без согласия ее обладателя. То есть «конфиденциальность потока сообщений означает, что никто, даже при наличии доступа к каналам передачи и узлам коммутации сети, не должен иметь возможности установить, какого типа и какие данные передаются пользователю или поступают от пользователя, а также объем пересылаемых данных и адреса назначения»[7].

Преломляя понятие конфиденциальности к информации, носителем которой является сигнал в РК, и рассматривая ее в отсутствии криптографических преобразований только с технической стороны, можно сказать следующее. Информация при данных условиях будет обладать таким свойством вне РТС. То есть получить информацию может любой абонент на приемной стороне, параметры РТС которого совпадают с параметрами передающей РТС, и находящийся в зоне действия передающей РТС. При этом согласие абонента передающей РТС для доступа к передаваемой ею информации не требуется. Следовательно, понятие конфиденциальности информации в РК применимо и коррелирует с понятием скрытности или разведзащищенности:

$$C = 1 - \rho_r = 1 - \rho_{ob}\,\rho_{st}\,\rho_{in}, \quad (3)$$

где: ρ_r – вероятность разведки параметров РТС, ρ_{ob} – вероятность обнаружения сигналов РТС, ρ_{st} – вероятность раскрытия структуры сигнала, ρ_{in} – вероятность раскрытия информации (смысла).

Доступность – состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Доступность информации в РК является условием для конфиденциальности. Если информация будет не доступна, то вопрос о конфиденциальности снимается. На первый взгляд доступность определяется предельной чувствительностью приемника и достаточным уровнем сигнала на его входе на фоне шумов и помех, то есть уровнем мощности принятого сигнала, при котором обеспечивается отношение

7 Воробьев Е. Г. Управляемая поляризация электромагнитных волн как средство повышения скрытности передачи информации // Информатика, управление и компьютерные технологии. Известия СПбГЭТУ «ЛЭТИ». 2014. № 9. С 44–49.

его к уровню шума, равное единице. Тогда доступность можно определить вероятностью наступления такого события:

$$D = \rho(Q = 1), \quad (4)$$

где: Q – отношение сигнал/шум на входе приемника.

Тот факт, что при условии уверенного приема сигнала РТС (выполнения условия доступности) информация может быть искажена, относится к понятию целостности информации.

Целостность – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на это право. В данном контексте понятие целостности схоже с понятием достоверности и определяется вероятностью искажения бита или символа:

$$S = 1 - \rho_{b(s)}, \quad (5)$$

где: $\rho_{b(s)}$ – вероятность ошибки на бит (символ).

Для того, чтобы увязать формулы (3)–(5), можно использовать формулу полной вероятности, аналогичную (1).

Разумеется, что данные метрики являются лишь предложением и могут быть усложнены (например, в виде представления конфиденциальности условной вероятностью). Логический вывод и описание информационных показателей защищенности информации в РК приведено с целью разрешения указанного во введении противоречия. Возможные пути решения в виде аналитического описания конфиденциальности, доступности и целостности информации в РК позволят установить взаимосвязь между защищенностью информации и параметрами различных уровней ЭМВОС РТС. Также это позволит нормативно определить некриптографические методы защиты информации в РК, проводить анализ таких методов и разрабатывать новые.

Анализ современных «некриптографических» методов защиты информации в радиоканалах

В настоящее время, учитывая указанную выше проблематику, к некриптографическим методам защиты информации в РК можно отнести классические методы обеспечения помехоустойчивости, имитоустойчивости и скрытности.

Имитоустойчивость, определяемая как защита от подмены или ввода ложной информации, может быть рассмотрена как защита от имитирующих помех[8]. Имитоустойчивости также посвящены работы [11, 12]. В [10] также подробно описаны «некриптографические» методы защиты информации в виде борьбы с помехами на различных уровнях приемной РТС.

Разделим данные методы на антенные методы, методы фильтрации, методы помехоустойчивого кодирования и сигнальные методы.

К антенным методам относятся методы компенсации помех, пространственной фильтрации и селекции, частотной селекции и поляризационной селекции.

Компенсация помех осуществляется за счет формирования провалов в диаграмме направленности в направлении прихода помехового сигнала.

Пространственная селекция осуществляется за счет формирования главных максимумов диаграммы направленности в направлении цели или источника сигнала, управления главными максимумами диаграммы направленности и управлением уровнями боковых лепестков [12, 13]. Эти функции основаны на методах решения задачи синтеза антенн и управления весовыми коэффициентами – комплексными амплитудами антенных решеток. Последняя функция АР базируется на основе теории адаптивных АР [13, 14].

Поляризационная селекция позволяет использовать управляемые поляризационные характеристики антенн для повышения качества приема сигналов [8, 10, 14]. Если антенны приемника и передатчика имеют одинаковую поляризацию, мощность принятого сигнала будет максимальной при прочих равных. Известно направление поляризационной модуляции сигнала, результаты которого могут быть использованы для обеспечения защищенности информации в РК. Данные методы позволяют использовать параметры поляризационного эллипса для кодирования информации. Сами параметры изменяют с помощью адаптивного процессора при условии выполнения антенны с круговой поляризацией.

Частотная селекция позволяет использовать антенну как частотный фильтр при соблюдении условия широкополосности. Необходимо обеспечить максимальную амплитуду сигнала на входе антенны при сканировании по частоте. Для этого необходимо учитывать амплитудно-частотную характеристику антенно-фидерного устройства.

Кратким выводом по антенным методам является заключение о том, что данные методы разработаны относительно недавно, в середине прошлого века, и по аналогии с цифровой связью сегодня находят физическую основу для реализации. Такой основой выступают цифровые антенные решетки и смарт-антенны [15], включающие в состав микроконтроллеры управления параметрами, схемы цифрового управления лучом и специальные вычислители на основе методов искусственного интеллекта. Результатом применения совокупности методов и технологий является высокий уровень мощности сигнала на входе приемника, дополнительное кодирование

8 Максимов М. В. Защита от радиопомех: под ред. М. И. Максимова. М.: Сов. радио, 1976. 496 с.

информации параметрами антенн, что позволяет на физическом уровне внести вклад в защиту информации в РК.

Методы фильтрации основаны на оптимизации и разработке алгоритмов управления фильтрами радиоприемных устройств. Суть методов состоит в приближении амплитудно-частотной характеристики фильтра к идеальной. Это позволяет повысить качество выделения полезного сигнала из сигнальной смеси, и в результате уменьшить количество ошибок на входе канального кодера. В качестве наиболее перспективных фильтров можно выделить адаптивный фильтр Калмана. Параметры фильтров, такие как крутизна и неравномерность АЧХ, частота среза АЧХ и порядок фильтра, оказывают косвенное влияние на достоверность принятой информации.

Методы помехоустойчивого кодирования дают вклад в защиту информации в РТС на канальном уровне ЭМВОС. Разнообразие данных методов и их модификаций достаточно велико и известно[9]. Следует заметить, что уменьшение исправление ошибок декодером можно связать с целостностью информации. Наиболее применяемыми в РК являются каскадные коды, состоящие из кодов, корректирующих одиночные ошибки и кодов, корректирующих групповые ошибки. Первые представлены кодами с низкой плотностью единиц в порождающей матрице (LDPC), а вторые представлены кодом Рида-Соломона и его модификациями.

Класс сигнальных методов можно отобразить методами изменения параметров сигнала на основе применения различных типов модуляции [16, 17], их модификаций, а также методов расширения спектра[10] [16]. Синтез широкополосных сигналов при разумных технических затратах на их реализацию позволяет осуществлять передачу информации на энергетическом уровне предела Шеннона, обеспечивая требуемую скрытность, что влияет на конфиденциальность информации в РК. Использование псевдослучайной перестройки рабочей частоты (ППРЧ) также позволяет обеспечить целостность и конфиденциальность информации в РК за счет скачков по поднесущим частотам и восстановлении информации в случае воздействия помехи в узкой полосе. Кроме того, традиционным подходом повышения скрытности передаваемой информации является скремблирование.

Необходимо отметить совмещение нескольких различных методов для достижения эмерджентных свойств РТС по защищенности информации в РК. Так, применение методов модуляции при разделении по ортогональным поднесущим частотам (OFDM – orthogonal frequency division modulation) в совокупности с методами на основе технологии MIMO (Multiple Input – Multiple Output) позволяет использовать в сочетании частотный и пространственный ресурс РК и реализовывать множество способов передачи, совмещая методы пространственного и частотного разнесения для повышения скрытности[11] [18]. На основе указанных методов в 2022 году утвержден стандарт передачи информации Wi-Fi 6.

Выводы

Таким образом, в работе проведен анализ нормативных документов по защите информации и радиосвязи для определения показателей защищенности информации в РК при использовании некриптографических методов ее защиты. Определено, что такие «информационные» показатели могут быть на основе логического вывода интерпретированы в показатели РТС, такие как скрытность, помехоустойчивость, имитостойкость и помехозащищенность. Либо может быть установлена аналитическая взаимосвязь между «информационными» и радиотехническими показателями. Так же на основании того, что определение «некриптографических» методов защиты информации в РК не дано ни в одном нормативном документе, то во второй части работы проведен неполный анализ радиотехнических методов, способных выступить в качестве таковых. Следует отметить, что методы оптимального приема, оптимальной фильтрации, оптимального кодирования, теории синтеза антенн и другие достаточно хорошо разработаны и описаны в научной литературе. Однако отличительной особенностью сегодняшнего научного развития является обострение междисциплинарного подхода, когда при проектировании лавинообразно увеличивающегося количества и видов радиотехнических систем невозможно четко разграничить защиту информации, радиотехнику, теорию автоматического управления, программирование микроконтроллеров, теорию цепей и технологии искусственного интеллекта. В связи с этим разработка новых методов защиты информации в РК на основе совмещения известных или заимствованных методов из других областей научного знания позволит внести значительный вклад в информационную безопасность.

9 Касами Т., Токура Н., Ивадари Ё., Инагаки Я. Теория кодирования: пер. с яп. М.: Мир, 1978. 568 с.

10 Борисов В. И. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты. М.: Радио и связь, 2000. 384 с.

11 Андронов, И. С., Финк Л. М. Передача дискретных сообщений по параллельным каналам. М. : Советское радио, 1971. 408 с.

Литература

1. *Мариненков Е. Д., Викснин И. И., Жукова Ю. А., Усова М. А. Анализ защищенности информационного взаимодействия группы беспилотных летательных аппаратов // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 5. С. 817–825. DOI: 10.17586/2226-1494-2018-18-5-817-825.*
2. *Головской В. А., Филинов В. С. Предложения по созданию когнитивных систем передачи данных для робототехнических комплексов // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. №9. С. 22–29.*
3. *Андреев А. М., Мальцев Г. Н., Федоренко М. Ю. Алгоритмы и аппаратура криптографической защиты информации в командных и телеметрических радиолиниях зарубежных космических систем // Успехи современной радиоэлектроники. 2018. № 4. С. 14–26.*
4. *Швиденко С. А., Иванов С. В., Хорольский Е. М., Савельев И. В. Один из эффективных подходов к защите информации в радиолиниях робототехнических комплексов с группами беспилотных летательных аппаратов на основе блокчейн технологии // Информатика, вычислительная техника и управление. 2022. Т.14. № 5. С. 21–26.*
5. *Коротков В. В., Мельников А. В. Актуальные вопросы информационной безопасности радиосвязи морского и речного транспорта // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. 2021. №12. С. 82–84. DOI: 10.37882/2223-2966.2021.12.14 2 (45).*
6. *Макаренко С. И. Информационный конфликт системы связи с системой дестабилизирующих воздействий. Часть. I: Концептуальная модель конфликта с учетом ведения разведки, физического, радиоэлектронного и информационного поражения средств связи // Техника радиосвязи. 2020. № 45. С. 104–117. DOI: 10.33286/2075-8693-2020-45-104-117.*
7. *Иванов М. А. Способ обеспечения универсальной защиты информации, пересылаемой по каналу связи // Вопросы кибербезопасности. 2019. № 3 (31). С. 45–50.*
8. *Макаренко С. И. Анализ средств и способов противодействия беспилотным летательным аппаратам. Часть 3. Радиоэлектронное подавление систем навигации и радиосвязи // Системы управления, связи и безопасности. 2020. № 2. С. 101–175. DOI: 10.24411/2410-9916-2020-10205.*
9. *Ватрухин Е. М. Комплексная защита информации в каналах «земля-борт» // Вестник Концерна ВКО «Алмаз-Антей». 2020. № 4. С. 6–14. DOI: 10.38013/2542-0542-2020-4-6-14.*
10. *Богатырев А. А., Ермолаев А. С., Саменков Е. В., Нуржанов Д. Х., Подсякина А. Ю. Физические принципы методов защиты от помех // Труды Международного симпозиума «Надежность и качество». 2018. Т. 2. С. 315–317.*
11. *Глобин Ю. О., Финько О. А. Способ обеспечения имитоустойчивой передачи информации по каналам связи // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 2. С. 30–43. DOI: 10.36724/2409-5419-2020-12-2-30-43.*
12. *Басан Е. С., Прошкин Н. А., Силин О. И. Повышение защищенности беспроводных каналов связи для беспилотных летательных аппаратов за счет создания ложных информационных полей // Сибирский аэрокосмический журнал. 2022. Т. 23, № 4. С. 657–670. DOI: 10.31772/2712-8970-2022-23-4-657-670.*
13. *Шмачилин П. А., Шумилов Т. Ю. Матричная диаграммообразующая схема цифровой антенной решётки // Труды МАИ. 2019. № 109. DOI: 10.34759/trd-2019-109-12*
14. *Ваганова А. А., Кисель Н. Н., Панычев А. И. Направленные и поляризационные свойства микрополосковой реконфигурируемой антенны, перестраиваемой по частоте и поляризации // Известия ЮФУ. Технические науки. 2021. № 2. С. 74–83. DOI: 10.18522/2311-3103-2021-2-74-83*
15. *Ma Y., Wang J., Li Y., Chen M., Li Z., Zhang Z. Smart antenna with automatic beam switching for mobile communication // EURASIP Journal on Wireless Communications and Networking. 2020. No. 179. Pp. 2–4. DOI: 10.1186/s13638-020-01792-4*
16. *Карпухин Е. О., Макаренков Н. С. Применение сигналов OCDM-OFDM с псевдослучайной перестройкой рабочей частоты для предотвращения атак на физическом уровне // Труды МАИ. 2019. № 106.*
17. *Khalifa M. A. E., Emam A. E., Youssef M. I. Performance enhancement of MIMO-OFDM using redundant residue number system // Advances in science, Technology and engineering systems journal. 2018. Vol. 3, No. 4. Pp. 1–7.*
18. *Elghany M. A., Emam A. E., Youssef M. I. ICI and PAPR enhancement in MIMO-OFDM system using RNS coding // International Journal of Electrical and Computer Engineering (IJECE). 2019. Vol. 9. No. 2. pp. 1209–1219. DOI: 10.11591/ijece.v9i2.pp1209-1219.*