СОЗДАНИЕ ИНТЕГРИРОВАННОЙ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Филин А. В.[1], Заикин Р. В.[2]

DOI:10.21681/3034-4050-2025-5-48-54

Ключевые слова: *система, инфотелекоммуникация, система опознавания, имитозащита.*

Аннотация

Цель работы *заключается в рассмотрении перспектив развития системы обеспечения информационной безопасности и системы опознавания пользователей в составе инфотелекоммуникационной системы специального назначения, а также исследовании приоритетных направлений, связанных с обеспечением безопасности связи.*

Метод исследования: *анализ, синтез исходных данных, постановка проблемы недостаточной эффективности существующей системы обеспечения информационной безопасности.*

Результаты исследования: *в ходе исследования была разработана модель системы обеспечения информационной безопасности, ее отдельные элементы, представлено место и роль в инфотелекоммуникационной системе специального назначения. Рассмотрены основные направления обеспечения информационной безопасности инфотелекоммуникационной системы специального назначения с учетом опыта СВО.*

Практическая полезность заключается в задании вектора развития системы обеспечения информационной безопасности с учетом опыта СВО, данная работа может стать опорой для дальнейших исследований в области информационной безопасности.

Введение

Полученный войсками в ходе специальной военной операции (СВО) опыт ещё раз подчеркивает, что обеспечение безопасности связи является одной из важных составных частей в общей системе мер по противодействию техническим средствам разведки противника и обеспечению скрытого управления войсками. Своевременный контроль радиоэлектронной обстановки и информационных потоков в беспроводных сетях передачи данных при наличии штатных средств позволит формировать объективные исходные данные по техническим демаскирующим признакам для планирования мероприятий оперативной маскировки. При этом перспективны удаленно управляемые средства радиоконтроля на базе SDR-технологии, а также средства сетевого контроля безопасности сетей передачи данных.

Органы контроля при наличии средств радиомониторинга могут решать задачу определения вариантов рационального использования радиочастотного ресурса, а также изучения порядка использования частотного ресурса противником для решения ряда задач по оповещению о приближении беспилотных летательных аппаратов (БПЛА) противника, и формированию ложной радиоэлектронной обстановки в рамках поставленных задач по оперативной маскировке. Возможность решения существующих и перспективных задач контроля безопасности связи в настоящее время зависит в большей степени не от средств добывания, а от средств обработки и квалификации персонала. Сложившаяся ситуация требует новых организационных и технических решений по обеспечению и контролю безопасности связи, особенно в связи со значительной глубиной «серой зоны».

По подсистеме узлового контроля необходимо проработать порядок взаимодействия с операторами связи с целью выявления фактов несанкционированного использования

1 Филин Андрей Викторович, заместитель начальника Военно-учебного центра политехнического университета имени Петра Великого, Санкт-Петербург. E-mail: fi1y@mail.ru

2 Заикин Руслан Валерьевич, курсант факультета АСУ Военной академии связи имени Маршала Советского Союза С. М. Буденного, Санкт-Петербург. E-mail: rus.zaikin.03@mail.ru

оконечных мультимедийных средств, обосновать типовой и количественный состав средств контроля для решения задач узлового контроля.

По сетевому контролю необходимо создание экспертной группы для выполнения задачи паспортизации связной инфраструктуры в районах проведения СВО. Результаты паспортизации должны быть детализированы с точностью, достаточной для решения следующих задач:

- своевременного выявления и пресечения действий технической компьютерной разведки и специальных программных воздействий;
- выбора безопасных маршрутов для организации и обеспечения связи;
- обоснование количества и типового состава средств связи, необходимых для использования ресурсов связной инфраструктуры в районах проведения СВО;
- формирования каталогов технических демаскирующих признаков типовых объектов для планирования мероприятий оперативной маскировки.

Повышение разведзащищенности пунктов управления (узлов связи) представляется возможным путем обеспечения мобильности и ослабления технических демаскирующих признаков за счет их своевременной фиксации, обработки и управления признаковым пространством.

Для повышения безопасности связи и разведзащищенности системы связи, а также обеспечения радиоэлектронной защиты узлов связи пунктов управления соединения необходимо дополнить систему управления соединения подсистемой контроля безопасности связи. Типовые технические решения по созданию аппаратных контроля безопасности связи применительно к условиям СВО не обеспечат требуемой эффективности и не позволят решать поставленные задачи.

Ближайшей перспективой развития инфотелекоммуникационной системы специального назначения (ИТКС СН) предусмотрено создание интегрированной системы обеспечения информационной безопасности [1].

Интегрированная система обеспечения информационной безопасности

Информационная безопасность ИТКС СН – состояние защищенности информационной сферы системы военной связи от заданного множества угроз информационной безопасности системы военной связи, в котором обеспечивается ее штатное функционирование. Информационная безопасность ИТКС СН определяется безопасностью связи, информационной безопасностью сетей связи и АСУ, информационной безопасностью узлов и линий связи (рис. 1).

Интегрированная система обеспечения информационной безопасности (СОИБ) ИТКС СН представляет собой совокупность служб и объектов информационной безопасности, механизмов обеспечения информационной безопасности ИТКС, органов управления и исполнителей, осуществляющих руководство, планирование и обеспечение информационной безопасности и функционирующих по правилам, установленным комплектом правовых, организационно-распорядительных и нормативных документов в области информационной безопасности ИТКС СН с целью сведения до минимума возможного ущерба ее пользователям [2].

Основными целями СОИБ при этом являются:

1) требуемая эффективность функционирования ИТКС СН при реализации угроз ИБ;
2) требуемая защищенность информационной сферы ИТКС СН;
3) непрерывность управления ИБ ИТКС СН.

Структура системы обеспечения информационной безопасности при этом включает подсистему безопасности связи, защищенную АСУС, подсистему мониторинга технического состояния средств связи и безопасности связи, подсистему безопасности сетей связи и АСУ и подсистему безопасности информации на узлах связи и в линиях связи.

Особую актуальность приобретает проблема обеспечения криптографическими ключами защищенных средств связи. В связи с высоким риском компрометации шифров на территории, ранее занимаемой противником запасы ключевых документов не создаются [3].

Опыт СВО подтверждает, что широкое внедрение программно-аппаратных средств в комплексах связи и управления оружием приводит к стиранию грани между средствами вычислительной техники (СВТ) и радиоэлектронными средствами (РЭС). Отсутствие четкой грани приводит к необходимости использовать термин «информационно-техническое средство» (ИТС). Этот термин является

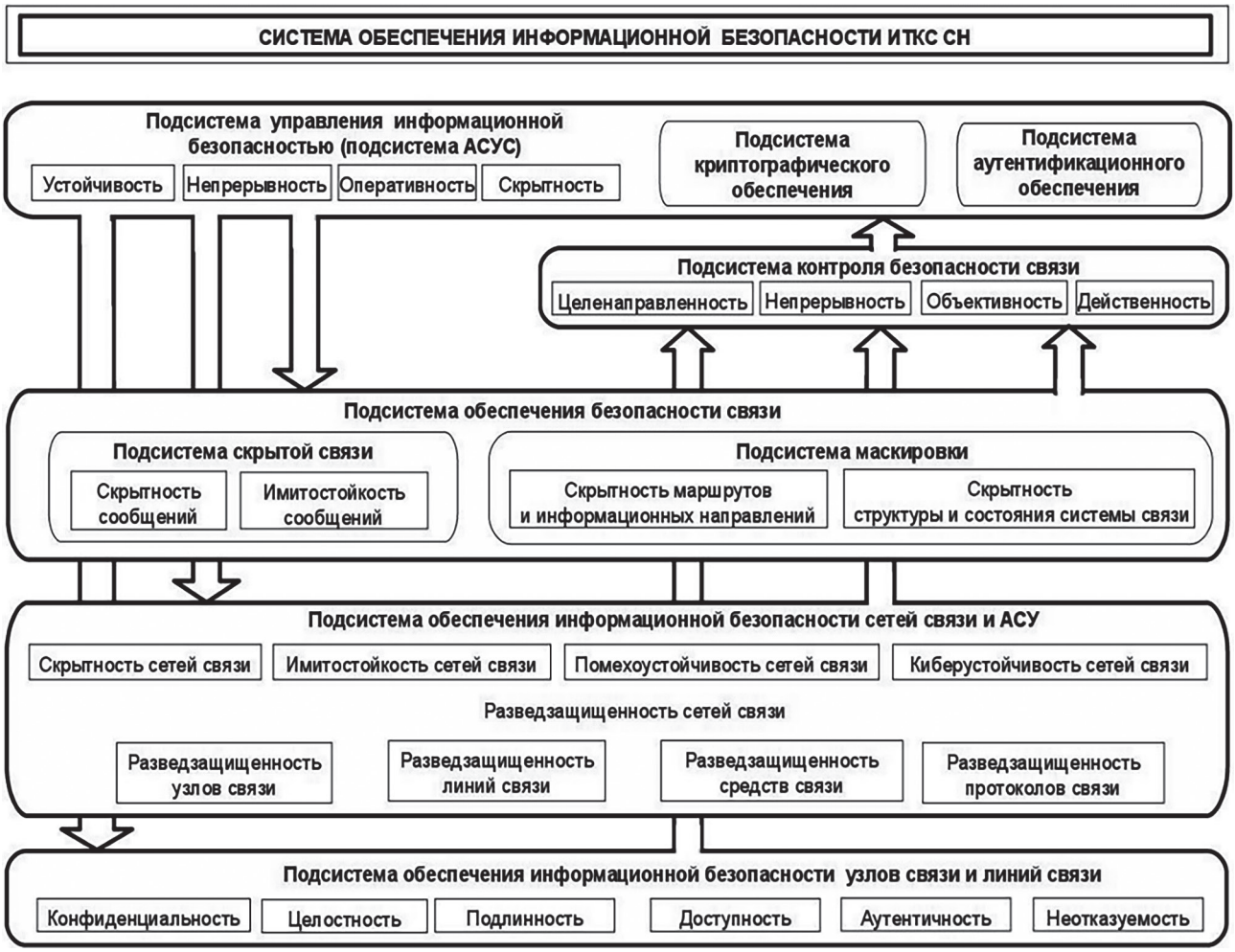

Рис. 1. Структура системы обеспечения информационной безопасности ИТКС СН

собирательным и обозначает любые РЭС, СВТ, а также их конструктивно единую комбинацию в форме робототехнических комплексов (РТК) [4].

Планы DARPA Минобороны США по переходу к полноценной робототехнической армии, увеличение дальности действия робототехнических комплексов военного назначения обусловливают повышение требований к надежности опознавания элементов системы связи и ИТС РТК. В связи с этим дальнейшая перспектива развития системы обеспечения информационной безопасности ИТКС СН связана с созданием системы опознавания пользователей и ИТС РТК.

Система опознавания пользователей (СОП) ИТКС СН предназначена для определения подлинности (принадлежности) пользователей и ресурсов (объектов) к ИТКС СН с целью предоставления доступа к ее услугам и ресурсам только зарегистрированных пользователей и объектов [5].

Определение подлинности пользователей и ресурсов ИТКС СН должно осуществляться на основе комплексного применения функциональных компонентов безопасности, подтверждающих подлинность свидетельств принадлежности пользователей и объектов ИТКС СН.

Основными функциональными компонентами безопасности, составляющими СОП, должны быть идентификация, аутентификация и авторизация [6]. К числу основных субъектов и объектов ИТКС СН должны быть отнесены: абоненты, должностные лица по связи, терминалы, сетевые устройства (серверы, коммутаторы, маршрутизаторы, выделенные и виртуальные сети, их элементы, физические и логические каналы, модемы, элементы робототехнических комплексов), прикладные

и управляющие программы и процессы, базы данных, файлы, данные.

СОП должна обеспечивать реализацию профиля защиты ИТКС СН от следующих угроз:

- раскрытия информации неавторизованному пользователю или процессу (утечка информации);
- использования ресурсов неавторизованным объектом или субъектом (незаконное использование);
- преднамеренной блокировки легального доступа к информации или другим ресурсам (отказ в услуге);
- искажение, ввод ложной информации, ввод дополнительной информации в системы управления робототехническими комплексами;
- подмена объектов или субъектов в системе управления робототехническими комплексами.

В целом СОП должна с заданной вероятностью гарантировать опознавание подлинности пользователя, источника данных (данных), сеанса связи пользователей, передаваемых сообщений и тем самым обеспечить требуемую имитозащищенность информационных процессов в ИТКС СН [7].

Имитозащита информационного процесса – это целевая функция защищенной организационно-технической системы по снижению вероятности или исключению возможности несанкционированного изменения состава или параметров используемых ИТС и биологических субъектов информационного процесса, искажению циркулирующей или вводу дополнительной информации [8].

Подсистема безопасности сетей связи и АСУ будет иметь типовые модули: криптозащиты, маскировки, защиты информации на узлах связи, защиты радиосетей и защиты сетей передачи данных (рис. 2).

Рис. 2. Структура подсистемы безопасности связи ИТКС ВН

Приоритетными направлениями исследований по обеспечению контроля безопасности связи в настоящее время являются:

- разработка модели уязвимостей и угроз безопасности для новых информационных технологий и объектов информационной инфраструктуры (в частности, для систем управления робототехническими комплексами военного назначения);
- создание автоматизированной подсистемы управления и контроля безопасности связи ВС;
- совершенствование способов сетевого контроля безопасности информации в цифровых сетях передачи данных;
- совершенствование нормативно-правовой базы по контролю безопасности связи [9].

С учетом опыта СВО основными задачами совершенствования подсистемы контроля безопасности связи являются:

- разработка типового варианта оборудования поста контроля безопасности связи для тактического звена управления, совершенствование алгоритмов обработки нарушений безопасности связи;
- разработка единой системы мониторинга информационной безопасности телекоммуникационного оборудования сетей передачи данных;
- разработка средств и систем поддержки принятия решений по управлению безопасностью связи с интеграцией в АСУ связью.

Ожидаемый эффект заключается в обеспечении повышения разведзащищенности системы связи и скрытности управления войсками за счет оперативности и точности контроля безопасности связи.

Приоритетными направлениями исследований по обеспечению закрытой связи в настоящее время являются:

- разработка защищенных сетевых протоколов, обеспечивающих скрытие криптотуннелей и безопасное дистанционное управление ключами шифрования;
- разработка унифицированной аппаратуры пакетного шифрования и фильтрации с программно-определяемой конфигурацией для обеспечения распределения обрабатываемой информации по мандатным меткам между криптотуннелями и возможности работы в туннельном или транспортном режимах при сопряжении сетей связи различных классов и ведомств;
- реализация функций граничного маршрутизатора и системы обнаружения атак в криптомаршрутизаторах;
- реализация функций генерации ложного трафика между внутренними маршрутизаторами криптомаршрутизатора [10].

С учетом опыта СВО основными задачами совершенствования криптографической защиты системы связи являются:

- разработка технологии безопасного дистанционного управления средствами криптографической защиты информации, встроенными в средства радиосвязи тактического звена управления;
- разработка средств пакетного шифрования для тактического звена управления в несекретном исполнении без ключевой информации и секретных составляющих криптосхем.

Заключение

В статье рассмотрены направления обеспечения информационной безопасности инфотелекоммуникационной системы специального назначения, с учетом опыта СВО. Выявлены особенности, которые приводят к изменению облика системы военной связи и превращают ее в информационно-телекоммуникационную систему. Требуют рассмотрения вопросы криптографического обеспечения в состав боевого обеспечения войск связи и совершенствование технологий обеспечения имитозащищенности информационных процессов для перспективной ИТКС СН, включающей средства связи и управления робототехническими комплексами военного назначения.

Литература

1. Иванов В. Г. и др. Проблемы построения и функционирования системы связи специального назначения в операции. Стратегическая стабильность. 2020. № 4 (93). С. 11–14.3.
2. Иванов В. Г. Основы построения и оценки эффективности функционирования системы связи специального назначения в международном вооруженном конфликте на основе многосферной и конвергентной структуры ее элементов: Монография. – СПб.: ПОЛИТЕХ, 2023. – 298 с.

3. Иванов В. Г., Филин А.В., Сарафанников В. С. [и др.] Обеспечение безопасности и устойчивости управления на основе развертывания виртуальных пунктов управления // Сборник статей II Всероссийской научно-технической конференции. ФГАУ «Военный инновационный технополис «ЭРА». – Анапа, 2020. – С. 263–269.
4. Николаева, М. О. Информационная безопасность: современная картина проблемы информационной безопасности и защиты информации / М. О. Николаева // Мониторинг. Образование. Безопасность. – 2023. – Т. 1, № 1. – С. 51-57. – EDN IOIQDI.
5. Евдокимов, О. Г. Подход к оценке эффективности системы обеспечения информационной безопасности распределенной системы передачи данных / О. Г. Евдокимов, Г. П. Гавдан, С. А. Резниченко // Безопасность информационных технологий. – 2022. – Т. 29, № 2. – С. 57–70. – DOI 10.26583/bit.2022.2.05. – EDN GQJYFN.
6. Болдырев, А. Н. Информационная безопасность. Виды угроз информационной безопасности / А. Н. Болдырев // Современные тенденции развития гуманитарных, правовых и экономических исследований Республики Калмыкия: теория и практика : Сборник материалов III Республиканской студенческой научно-практической конференции, Элиста, 18 марта 2021 года. – Элиста: Калмыцкий филиал федерального государственного бюджетного образовательного учреждения инклюзивного высшего образования «Московский государственный гуманитарно-экономический университет», 2021. – С. 137–140. – EDN IWIEGE.
7. Лебедев, Д. В. Анализ данных об угрозах информационной безопасности для формирования комплексной системы информационной безопасности / Д. В. Лебедев // Весенние дни науки : Сборник докладов международной конференции студентов и молодых ученых, Екатеринбург, 20–22 апреля 2023 года. – Екатеринбург: ООО Издательский Дом «Ажур», 2023. – С. 58–62. – EDN IWNQLI.
8. Качан, Я. С. Проектирование системы защиты для обеспечения безопасности критической информационной инфраструктуры / Я. С. Качан // Научные исследования 2024 : Сборник статей XI Международной научно-практической конференции. В 2-х частях, Пенза, 12 июня 2024 года. – Пенза: Международный центр научного сотрудничества «Наука и Просвещение», 2024. – С. 89–92. – EDN ILTQWM.
9. Гуменюк, Н. В. Методологические подходы оценки рисков информационной безопасности / Н. В. Гуменюк, А. Д. Катунин // Научно-технические аспекты развития автотранспортного комплекса : Материалы X Международной научно-практической конференции, в рамках 10-го Международного научного форума Донецкой Народной Республики, Горловка, 31 мая 2024 года. – Горловка: Донецкий национальный технический университет, 2024. – С. 495–499. – EDN XNADOR.
10. Канзюба, Е. Д. Обеспечение информационной безопасности и киберустойчивости телекоммуникационных систем, автоматизированных систем управления / Е. Д. Канзюба // ЭНЕРГОСТАРТ : Материалы VI Международной молодежной научно-практической конференции в рамках Десятилетия науки и технологий в Российской Федерации, Кемерово, 17–22 ноября 2023 года. – Кемерово: Кузбасский государственный технический университет им. Т. Ф. Горбачева, 2023. – С. 405-1. – EDN PBYWAK.

CREATION OF AN INTEGRATED INFORMATION SECURITY SYSTEM FOR A SPECIAL-PURPOSE INFOTELECOMMUNICATION SYSTEM

Filin A. V.[3], Zaikin R. V.[4]

Keywords: *system, infotelecommunications, identification system, imitation protection.*

Abstract

The purpose of the work *is to consider the prospects for the development of the information security system and the user identification system as part of a special-purpose information telecommunication system, as well as to study the priority areas related to ensuring the security of communications.*

3 Andrey V. Filin, Deputy Head of the Military Training Center of Peter the Great Polytechnic University, St. Petersburg. E-mail: fi1y@mail.ru
4 Ruslan V. Zaikin, cadet of the Faculty of Automated Control Systems of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny, St. Petersburg. E-mail: rus.zaikin.03@mail.ru

Research method: *analysis, synthesis of initial data, formulation of the problem of insufficient efficiency of the existing information security system.*

Results of the study: *in the course of the study, a model of the information security system, its individual elements were developed, the place and role in the special purpose info telecommunication system were presented. The main directions of ensuring the security of the special purpose info telecommunication system were considered, taking into account the experience of the special military operation.*

Practical usefulness *lies in setting the vector for the development of the information security system, considering the experience of the special military operation, this work can become a support for further research in the field of information security.*

References

1. Ivanov V. G. i dr. Problemy postroenija i funkcionirovanija sistemy svjazi special'nogo naznachenija v operacii. Strategicheskaja stabil'nost'. 2020. № 4 (93). S. 11–14.3.
2. Ivanov V. G. Osnovy postroenija i ocenki jeffektivnosti funkcionirovanija sistemy svjazi special'nogo naznachenija v mezhdunarodnom vooruzhennom konflikte na osnove mnogosfernoj i konvergentnoj struktury ee jelementov: Monografija. – SPb.: POLITEH, 2023. – 298 s.
3. Ivanov V. G., Filin A. V., Sarafannikov V. S. [i dr.] Obespechenie bezopasnosti i ustojchivosti upravlenija na osnove razvertyvanija virtual'nyh punktov upravlenija // Sbornik statej II Vserossijskoj nauchno-tehnicheskoj konferencii. FGAU «Voennyj innovacionnyj tehnopolis «JeRA». – Anapa, 2020. – S. 263–269.
4. Nikolaeva, M. O. Informacionnaja bezopasnost': sovremennaja kartina problemy informacionnoj bezopasnosti i zashhity informacii / M. O. Nikolaeva // Monitoring. Obrazovanie. Bezopasnost'. – 2023. – T. 1, № 1. – S. 51–57. – EDN IOIQDI.
5. Evdokimov, O. G. Podhod k ocenke jeffektivnosti sistemy obespechenija informacionnoj bezopasnosti raspredelennoj sistemy peredachi dannyh / O. G. Evdokimov, G. P. Gavdan, S. A. Reznichenko // Bezopasnost' informacionnyh tehnologij. – 2022. – T. 29, № 2. – S. 57–70. – DOI 10.26583/bit.2022.2.05. – EDN GQJYFN.
6. Boldyrev, A. N. Informacionnaja bezopasnost'. Vidy ugroz informacionnoj bezopasnosti / A. N. Boldyrev // Sovremennye tendencii razvitija gumanitarnyh, pravovyh i jekonomicheskih issledovanij Respubliki Kalmykija: teorija i praktika : Sbornik materialov III Respublikanskoj studencheskoj nauchno-prakticheskoj konferencii, Jelista, 18 marta 2021 goda. – Jelista: Kalmyckij filial federal'nogo gosudarstvennogo bjudzhetnogo obrazovatel'nogo uchrezhdenija inkljuzivnogo vysshego obrazovanija «Moskovskij gosudarstvennyj gumanitarno-jekonomicheskij universitet», 2021. – S. 137–140. – EDN IWIEGE.
7. Lebedev, D. V. Analiz dannyh ob ugrozah informacionnoj bezopasnosti dlja formirovanija kompleksnoj sistemy informacionnoj bezopasnosti / D. V. Lebedev // Vesennie dni nauki : Sbornik dokladov mezhdunarodnoj konferencii studentov i molodyh uchenyh, Ekaterinburg, 20–22 aprelja 2023 goda. – Ekaterinburg: OOO Izdatel'skij Dom «Azhur», 2023. – S. 58-62. – EDN IWNQLI.
8. Kachan, Ja. S. Proektirovanie sistemy zashhity dlja obespechenija bezopasnosti kriticheskoj informacionnoj infrastruktury / Ja. S. Kachan // Nauchnye issledovanija 2024 : Sbornik statej XI Mezhdunarodnoj nauchno-prakticheskoj konferencii. V 2-h chastjah, Penza, 12 ijunja 2024 goda. – Penza: Mezhdunarodnyj centr nauchnogo sotrudnichestva «Nauka i Prosveshhenie», 2024. – S. 89–92. – EDN ILTQWM.
9. Gumenjuk, N. V. Metodologicheskie podhody ocenki riskov informacionnoj bezopasnosti / N. V. Gumenjuk, A. D. Katunin // Nauchno-tehnicheskie aspekty razvitija avtotransportnogo kompleksa : Materialy X Mezhdunarodnoj nauchno-prakticheskoj konferencii, v ramkah 10-go Mezhdunarodnogo nauchnogo foruma Doneckoj Narodnoj Respubliki, Gorlovka, 31 maja 2024 goda. – Gorlovka: Doneckij nacional'nyj tehnicheskij universitet, 2024. – S. 495–499. – EDN XNADOR.
10. Kanzjuba, E. D. Obespechenie informacionnoj bezopasnosti i kiberustojchivosti telekommunikacionnyh sistem, avtomatizirovannyh sistem upravlenija / E. D. Kanzjuba // JeNERGOSTART : Materialy VI Mezhdunarodnoj molodezhnoj nauchno-prakticheskoj konferencii v ramkah Desjatiletija nauki i tehnologij v Rossijskoj Federacii, Kemerovo, 17–22 nojabrja 2023 goda. – Kemerovo: Kuzbasskij gosudarstvennyj tehnicheskij universitet im. T.F. Gorbacheva, 2023. – S. 405-1. – EDN PBYWAK.