ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056

DOI: 10.21822/2073-6185-2025-52-1-57-66 Обзорная статья/ Review article

К вопросу об усовершенствовании систем безопасности критически важных объектов, как объектов критической информационной инфраструктуры

А.А. Гавришев
Национальный исследовательский ядерный университет «МИФИ»,
115409, г. Москва, Каширское шоссе, д. 31, Россия,
Московский государственный лингвистический университет»,
119034, г. Москва, Остоженка 38, стр. 1, Россия

Резюме. Цель. Целью данной статьи является выявление путей усовершенствования систем безопасности (СБ) критически важных объектов (КВО), подпадающих под регулирование законодательства о критической информационной инфраструктуре (КИИ). **Метод.** Использованы методы защиты информации и информационной безопасности, анализа и обобщения отдельных положений нормативно-правовых документов по обеспечению ИБ объектов КИИ, результаты научно-исследовательских работ по тематике исследования, представленные в РИНЦ, РГБ, ФИПС. Общей методологической основой является системный подход**. Результат.** Проведен обзор требований нормативно-правовых документов по обеспечению безопасности СБ КВО, как объектов КИИ, показавший, что необходим анализ сложившейся практики обеспечения их безопасности. Проведен обзор методов обеспечения безопасности радиоканальных СБ КВО, присутствующих на рынке России. В качестве примера рассматривались широко используемые радиоканальные системы охранной сигнализации (СОС). Выявлены противоречия между отдельными положениями нормативно-правовых документов по обеспечению безопасности объектов КИИ и сложившейся практикой применения радиоканальных СБ КВО, которые возможно отнести к объектам КИИ. С учетом введённых упрощений, предложены возможные пути усовершенствования СБ КВО, которые могут быть отнесены к незначимым объектам КИИ, в частности радиоканальные СОС. **Вывод**. Проведенные исследования позволили выявить пути усовершенствования радиоканальных СБ КВО, как объектов КИИ, в области обеспечения их ИБ.

Ключевые слова: критически важные объекты, критическая информационная инфраструктура, системы безопасности, информационная безопасность, усовершенствование

Для цитирования: А.А. Гавришев. К вопросу об усовершенствовании систем безопасности критически важных объектов, как объектов критической информационной инфраструктуры. Вестник Дагестанского государственного технического университета. Технические науки. 2025; 52(1):57-66. DOI:10.21822/2073-6185-2025-52-1-57-66.

On the issue of improving the security systems of critical facilities as objects of critical information infrastructure

A.A. Gavrishev
National Research Nuclear University MEPHI,
31 Kashirskoe highway, Moscow 115409, Russia,
Moscow State Linguistic University,
38 Ostozhenka St., build. 1, Moscow 119034, Russia

Abstract. Objective. The purpose of this article is to identify ways to improve the security systems (SS) of critical facilities (CF) that are subject to the regulation of legislation on critical information infrastructure (CII). **Method.** The methods used were information protection and information security, analysis and generalization of individual provisions of regulatory docu-

ments on ensuring the information security of critical information infrastructure facilities, the results of research work on the subject of the study, presented in the Russian Science Citation Index, Russian State Library, and Federal Institute of Industrial Property. The general methodological basis is a systematic approach. **Result.** A review of the requirements of regulatory and legal documents on ensuring the safety of the SS of CF, as objects of CII, has been conducted, which showed that an analysis of the established practice of ensuring their safety is necessary. A review of the methods of ensuring the safety of radio-channel SS present in the Russian market is carried out. Widely used radio channel security alarm systems (SAS) are considered. Contradictions have been revealed between certain provisions of regulatory legal documents on ensuring the safety of CII and the established practice of using radio-channel SS, which can be attributed to CII. Ways to improve the security system of critical information systems, which can be classified as insignificant critical information infrastructure objects, in particular radio channels alarm systems. **Conclusion.** The conducted research allowed us to identify ways to improve the radio-channel SS of the CF, as objects of CII, in the field of ensuring their IS.

Keywords: critical facilities, critical information infrastructure, security systems, information security, improvement.

For citation: A.A. Gavrishev. On the issue of improving the security systems of critical facilities as objects of critical information infrastructure. Herald of the Daghestan State Technical University. Technical Sciences. 2025; 52(1):57-66. (In Russ) DOI:10.21822/2073-6185-2025-52-1-57-66

Введение. Тенденции последнего времени показывают, что вопросам обеспечения безопасности критически важных объектов (КВО) стало уделяться повышенное внимание. Статические данные показывают [1], что КВО в мире и в России становятся объектом сравнительно небольшого числа различных, в том числе и террористических, атак (примерно 10 % от общего числа). Однако последствия этих атак могут быть очень серьезными. В указанных условиях, для обеспечения устойчивого функционирования КВО при проведении в отношении них различных атак, на таких объектах должны быть созданы системы безопасности (СБ) различного назначения, призванные обеспечить безопасность персонала КВО, противодействовать террористическим и криминальным угрозам и т.д. Такие системы обычно включают в себя следующие широко распространённые системы: системы охранной сигнализации (СОС), системы контроля и управления доступа (СКУД), системы охранного телевидения (СОТ) и некоторые другие. Указанные системы обычно являются составными частями общей физической защиты КВО [2-5], поэтому они играют большую роль в обеспечении безопасности КВО. Вместе с тем, в условиях непрерывной информатизации всех сфер хозяйственной деятельности человека, такие процессы не проходят бесследно, как для КВО в целом, так и для СБ в частности. Так в настоящее время на КВО зачастую для обеспечения передачи данных в различных системах, например [3-6], в системах охраны периметра или системах контроля доступа, применяются системы радиосвязи.

С учетом сказанного и источников [2-5], заключим, что современные СБ представляют собой сложные программно-аппаратные комплексы и по своей сути являются объектами информатизации. Согласно ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения», под такими объектами обычно подразумевается совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов, в которых эти средства и системы установлены. Несомненно, что СБ так же к ним относятся. Исходя из этого, возможно заключить, что КВО имеют в своем составе, помимо многочисленных информационных систем, автоматизированных систем управления и прочих, отвечающих за управление специфическими технологическими процессами

объекта, так же и многочисленные системы, выполняющие важные вспомогательные функции, связанные с обеспечением безопасности, в частности СБ [5, 7].

Вместе с тем, в последние годы, в условиях информатизации, на первое место вышла проблема обеспечения информационной безопасности (ИБ) многочисленных информационных систем, автоматизированных систем управления и прочих, отвечающих за управление специфическими технологическими процессами, входящих в состав КВО, как объектов критической информационной инфраструктуры (КИИ) [7, 8].

Однако до настоящего времени обеспечение ИБ самих СБ КВО, как объектов информатизации, не рассматривалось широко в литературе, что может негативно сказаться на функционировании КВО при проведении против них различных атак. Один из важных шагов в указанном направлении был сделан в начале 2024 года [9], когда отдельные СБ КВО были отнесены к объектам КИИ, в частности СОС, СКУД и некоторые другие. Поэтому исследования обеспечения ИБ СБ КВО является актуальным направлением исследований и требует дальнейшей проработки.

Постановка задачи. Целью исследования является определение путей усовершенствования СБ КВО, подпадающих под регулирование законодательства о КИИ.

Задачей исследования является выявление противоречий между требованиями нормативно-правовых документов по обеспечению безопасности объектов КИИ и сложившейся практикой применения СБ КВО, которые возможно отнести к объектам КИИ.

Методы исследования. В начале 2024 года ситуация по обеспечению ИБ самих СБ КВО значительно изменилась, так как уполномоченные Федеральные органы исполнительной власти, по согласованию со ФСТЭК РФ, начали утверждать перечни типовых объектов КИИ, функционирующих в соответствующих сферах, подпадающих по регулирование законодательством о КИИ. Так Минпромторгом РФ был утвержден перечень типовых объектов КИИ РФ, функционирующих, например, в области химической промышленности [9]. В соответствии с принятыми нормативными документами к объектам КИИ впервые стали относиться системы безопасности КВО, в частности СОС и СКУД и некоторые другие. Фрагмент соответствующей таблицы приведен ниже (табл. 1).

Таблица 1. Пример систем безопасности КВО, отнесённые к объектам КИИ
Table 1. An example of the security systems of the CIO, related to the objects of the CII

№	Название типового объекта КИИ Name of a typical critical information infrastructure object	Осуществляемые критические процессы Critical processes being carried out
1.	СОС	Обнаружение проникновения и подача сигналов оповещения и извещения о проникновениях Detection of intrusion and provision of intrusion warning and notification signals
2.	СКУД	Управление доступом на территорию Access control to the territory

Как пояснили в Минпромторге РФ, информационные системы и автоматизированные системы управления из таких перечней – это основа для процедуры категорирования объектов КИИ в этих отраслях. Известно [8, 10], что основными мероприятия в рамках реализации обеспечения безопасности объектов КИИ являются следующие:

1. Категорирование объектов КИИ, в рамках реализации которого выделяются значимые объекты КИИ;
2. Выполнение требований по обеспечению безопасности объектов КИИ в зависимости от их категории значимости;
3. Информирование уполномоченных государственных органов о компьютерных инцидентах на объектах КИИ, произошедших, в том числе, и в результате компьютерных атак, и реагирование на них.

Из отдельных положений нормативно-правовых документов известно [8, 10], что в результате процесса категорирования объекту КИИ может быть установлена одна

из трех категорий значимости. Тогда он называется значимым объектом КИИ (ЗОКИИ). Либо, если объект КИИ не соответствует критериям значимости, ему не присваивается ни одна из таких категорий и такой объект называется незначимым объектом КИИ (НОКИИ). Организации, которым принадлежат, как ЗОКИИ, так и НОКИИ, обязаны соблюдать требования по обеспечению безопасности таких объектов КИИ, установленные соответствующим законодательством [11-13]. При этом требования по обеспечению безопасности объектов КИИ зависят от их категории значимости – чем выше категория значимости объекта КИИ, тем более строгие требования по обеспечению безопасности выдвигаются для них. Таким образом, в случае если СОС, СКУД и другие СБ, входящие в состав КВО, признаны ЗОКИИ или НОКИИ, то на них распространяются соответствующие требования законодательства. Исходя из этого, возникает ряд сложностей при обеспечении безопасности СОС, СКУД и других СБ, входящих в состав КВО, как объектов КИИ.

В связи с большой трудоемкостью процесса обеспечения безопасности объектов КИИ, в первую очередь значимых, далее рассмотрим упрощенный сценарий, при котором СБ КВО не будет присваивается ни одна из категорий значимости, и они будут НОКИИ. При реализации указанного сценария, не вдаваясь в подробности самого процесса категорирования, необходимо выполнять ряд обязательных требований, установленных законодательством о КИИ для НОКИИ [11-13]. Их условно возможно разделить на организационно-правовые и технические.

Организационно-правовые меры обеспечения безопасности НОКИИ, описанные в соответствующих нормативно-правовых документах, например, назначение заместителя руководителя, ответственного за обеспечение ИБ в организации; организационные меры по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты на таких объектах и другие, в целом не вызывают затруднений при их внедрении. При этом обязательные технические мероприятия по обеспечению безопасности НОКИИ в текущем законодательстве не определены и, согласно нормативно-правовым документам, могут определяться собственником НОКИИ самостоятельно, с учетом текущего законодательства. Вместе с тем, возможно предположить, что обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты на объектах КИИ, как одно из важных направлений обеспечения их безопасности, потребует наличия у организации, которая ими владеет, программных, программно-аппаратных и иных средств, с помощью которых возможно выполнить указанные функции.

Согласно ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения», известно, что под такими средствами понимаются технические, программные, программно-аппаратные и иные средства для обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также технические, программные, программно-аппаратные и иные средства поиска признаков компьютерных атак (СППКА) в сетях электросвязи и средства обмена информацией, для которых имеется документальное подтверждение соответствия требованиям, установленным в нормативных правовых актах и методических документах. Более их подробное описание приведено в ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения». В целом возможно заключить, что средства для обнаружения, предупреждения и ликвидации последствий компьютерных атак представляют собой обширный класс технических, программных и программно-аппаратных средств, призванных выполнять возложенные на них функции, с учетом нормативных ограничений законодательства. В силу своей многочисленности и обширности в отдельной статье не представляется возможным полностью охватить всю указанную область. Поэтому далее остановимся на СППКА в сетях электросвязи. СППКА в сетях электросвязи – это средства, предназначенные для обнаружения в сетях электросвязи, используемых для организации взаимодействия информационных ресурсов, признаков компьютерных атак по значениям

служебных полей протоколов сетевого взаимодействия, а также осуществления сбора, накопления и статистической обработки результатов такого обнаружения.

Согласно ГОСТ Р 53111-2008 «Устойчивость функционирования сети электросвязи. Требования и методы проверки», 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. Таким образом, в СБ КВО, отнесенных к НОКИИ, одним из самых важных мест является используемая система передача данных, независимо от того проводная она или нет. Вместе с тем, приведенные выше данные о внедрении систем радиосвязи в СБ, например в СОС, а также различные исследования показывают [3, 14-18], что для эффективного контроля больших территорий перспективным направлением является использованием радиоканальных СОС, обеспечивающих сбор информации с распределенных по территории объекта датчиков с радиоизвещением.

Датчики в данном случае располагаются по всей территории охраняемого объекта таким образом, чтобы расстояние между ними не превышало радиуса действия датчика, при котором обеспечивается обнаружение постороннего объекта и не образуются так называемые мертвые зоны. При попадании в зону действия датчика человека или постороннего предмета датчик фиксирует факт возникновения внештатной ситуации и посылает по радиоканалу на пульт управления системой сигнал тревоги. При этом передаваемые сигналы таких систем обеспечивают пространственную электромагнитную доступность, создающую благоприятные условия для реализации злоумышленниками различных угроз безопасности с помощью технических средств радиоразведки [3, 5, 14-18]. При этом, статистические данные, представленные НИЦ «Охрана» Росгвардии РФ [17], показывают, что около половины случаев нарушения работоспособности СБ КВО приходится на их каналы связи, в первую очередь беспроводные, и одними из основных преднамеренных угроз безопасности являются подмена передаваемых данных и постановка помех. Указанные факты, в условиях необходимости поиска признаков компьютерных атак в сетях электросвязи, ставят вопросы об углубленных исследования СБ КВО, отнесенных к объектам КИИ. Исходя из этого возникает задача анализа сложившейся практики обеспечения безопасности СБ КВО, которые возможно отнести к объектам КИИ.

Обсуждение результатов. Проведем обзор методов обеспечения безопасности радиоканальных СБ КВО, присутствующих на рынке России. Для дальнейших исследований будем рассматривать область защиты данных, передаваемых в радиоканальных СОС. Для этого обратимся к источникам [14-16, 19-23], в которых проанализированы некоторые широко используемые радиоканальные СОС.

В табл. 2 приведены характеристики некоторых из них. Как видно из табл. 2, в целом в радиоканальных СОС, присутствующих на рынке России, используются отдельные элементы защиты данных, передаваемых в радиоканале. При этом следует обратить внимание на следующие аспекты их применения:

1) Для работы с достаточно сложным оборудованием в области обеспечения ИБ необходимо наличие квалифицированного персонала с соответствующим опытом работы;

2) Ситуация, в рамках которой многие производители СБ используют сигналы с одним и тем же видом манипуляцией при передаче информации по радиоканалу [14, 19, 20, 23], является потенциальной уязвимостью и поэтому существует потребность в расширении арсенала используемых средств построения сигнально-кодовых конструкций;

3) Методы защиты передаваемой информации в радиоканальных СОС в целом возможно разделить на криптографические средства защиты информации, применяемые чаще всего, и технологии на основе шумоподобных сигналов, применяемые значительно реже [5, 14-18, 23];

4) Во многих радиоканальных СОС не указан прямо, какой алгоритм шифрования применяется, либо используются иностранные алгоритмы шифрования;

5) Многие радиоканальные СОС в целом не могут противостоять угрозам перехвата передаваемых данных и преднамеренного подавления их помехами в силу использования систем связи с простыми сигналами.

Таблица 2. Характеристики некоторых широко используемых радиоканальных СОС
Table 2. Characteristics of some widely used radio channel SAS

Название Name	**Диапазон рабочих частот, МГц Operating frequency range**	**Вид модуляции Modulation type**	**Использование шифрования Using encryption**	**Использование шумоподобных сигналов Using noise-like signals**
Стрелец-Аргон Sagittarius-Argon	146 – 174, 403 – 470	ЧМ	Да (алгоритм не указан) Yes (algorithm not specified)	Нет No
Базальт Basalt	450 – 453, 460 – 463	ЧМ	Да (алгоритм не указан) Yes (algorithm not specified)	ППРЧ
Приток-А-Р Pritok-A-R	136 – 174, 430 – 470	ЧМ	AES128	Нет No
Протон Proton	146 – 174, 403 – 470	ЧМ	Элементы криптозащиты Elements of cryptographic protection	Прямое расширение спектра с помощью кодов Баркера Direct Spread Spectrum with Barker Codes
Радиосеть Radio Network	450 – 453, 460 – 463	ЧМ	Элементы криптозащиты Elements of cryptographic protection	Нет No
Гермес Hermes	146 –174	ЧМ	Элементы криптозащиты Elements of cryptographic protection	ППРЧ
Астра-Зитадель Astra-Zitadel	2400 – 2480	Квадратурная ФМ Quadrature FM	Да (алгоритм не указан) Yes (algorithm not specified)	Прямое расширение спектра Direct Spread Spectrum

Таким образом, в целом следует признать, что современные радиоканальные СОС не в полной мере обеспечивают защиту передаваемых данных от известных угроз безопасности, например, перехвата передаваемого сигнала, его подмены или подавления помехами [14-18, 23]. Обзор нормативно-правовых требований по обеспечению безопасности самих СБ, как объектов КИИ, и методов обеспечения безопасности радиоканальных СБ, присутствующих на рынке России, показывает, что между ними существуют некоторые противоречия, в частности:

1. Средства поиска признаков компьютерных атак в сетях электросвязи для радиоканальных СБ в настоящий момент пока еще широко не описаны в литературе по таким системам;
2. Отсутствуют требования по обеспечению конфиденциальности, целостности и доступности передаваемых данных в радиоканале СБ;
3. Использование иностранных алгоритмов шифрования для обеспечения безопасности передачи данных в СБ КВО, как объектах КИИ, вступает в противоречие с требованиями законодательства об использовании отечественных алгоритмов шифрования [24];
4. Одним из регуляторов в области законодательного и технического регулирования для СБ в России является Росгвардия России, однако до настоящего времени ее роль для таких систем, отнесенных к КИИ, нормативно не урегулирована.

В связи с вышеизложенным, с учетом описанных замечаний и работ [3, 5, 14-23], выявлены следующие возможные пути усовершенствования СБ КВО, которые могут быть отнесены к незначимым объектам КИИ, в частности радиоканальные СОС:

1. Руководящие документы по обеспечению безопасности объектов КИИ, в качестве которых выступают различные радиоканальные системы, в частности СБ, целесообразно дополнить следующими угрозами безопасности: перехват передаваемых сигналов, подмена передаваемых сигналов и подавление их помехами;
2. Анализ различных источников [5, 14-23, 25, 26] показывает, что в качестве мер, направленных на поиск признаков компьютерных атак в сетях электросвязи, представленных радиосистемами, для СБ в настоящее время возможно использовать элементы криптографической защиты информации (электронная подпись, хэш-функции, имитовставки), технологии на основе шумоподобных сигналов, интеллектуальные методы поиска атак, аппарат нечёткой логики, аппарат сетей Петри и некоторые другие;
3. Для одновременного обеспечения конфиденциальности, целостности и доступности передаваемых данных в СБ КВО, необходимо применять технологии на основе шумоподобных сигналов, либо сочетание криптографических средств защиты информации и технологий на основе шумоподобных сигналов [3, 5, 14-19, 23];
4. Для обеспечения безопасности СБ КВО, как объектов КИИ, необходимо в обязательном порядке, при соблюдение установленных законодательством правил и процедур, использовать сертифицированные средства защиты информации из числа рекомендованных ФСБ РФ и ФСТЭК РФ [5, 14, 15, 24];
5. В соответствии с действующими нормативными требованиями [11], в СБ КВО, отнесенных к НОКИИ, запрещается использовать, за исключением оговоренных случаев, программные, программно-аппаратные и иные средства поиска признаков компьютерных атак в сетях электросвязи и защиты информации, странами происхождения которого являются, совершающие в отношении России недружественные действия. Исходя из этого, производителям СБ и их эксплуатантам, в случае отнесения таких объектов к КИИ, необходимо перейти на отечественные программные, программно-аппаратные и иные средства поиска признаков компьютерных атак в сетях электросвязи и защиты информации, либо произведенные в дружественных странах;
6. Целесообразно уточнить область технического регулирования СБ, отнесенных к КИИ.

Вывод. В данной статье приведены результаты исследования вопросов обеспечения ИБ систем безопасности КВО, как объектов КИИ.

Проведен обзор нормативно-правовых требований по обеспечению безопасности самих СБ КВО, как объектов КИИ, показавший, что необходим анализ сложившейся практики обеспечения безопасности СБ КВО, которые возможно отнести к объектам КИИ. Проведен обзор методов обеспечения безопасности радиоканальных СБ КВО, присутствующих на рынке России.

В качестве примера рассматривались широко используемые радиоканальные СОС. Показано, что современные радиоканальные СОС, как один из видов СБ, не в полной мере обеспечивают защиту передаваемых данных от известных угроз безопасности, например, перехвата передаваемого сигнала, его подмены или подавления помехами.

Выявлены противоречия между требованиями нормативно-правовых документов по обеспечению безопасности объектов КИИ и сложившейся практикой применения СБ КВО, которые возможно отнести к объектам КИИ.

С учетом введённых упрощений, предложены возможные пути усовершенствования СБ КВО, которые могут быть отнесены к незначимым объектам КИИ, в частности радиоканальные СОС.

Библиографический список:

1. Степанова, Е. Терроризм как угроза критической инфраструктуре / Е. Степанова // Свободная мысль. – 2010. – № 4. – С. 35-48.

2. Lawrence, Fennelly Effective Physical Security / Lawrence Fennelly. 2013. 4th Edition. Butterworth-Heinemann. – 366 P.
3. Кузьмина, Н.А. Системы фиксации и распознавания несанкционированного проникновения в охраняемую зону как элемент эффективной безопасности объекта транспортной инфраструктуры / Н.А. Кузьмина // T-Comm: Телекоммуникации и транспорт. – 2018. – Т. 12. – № 5. – С. 47-52. DOI: 10.24411/2072-8735-2018-10086
4. Волхонский, В.В. Особенности разработки структуры средств обнаружения угроз охраняемому объекту / В.В. Волхонский, А.Г. Крупнов // Научно-технический вестник информационных технологий, механики и оптики. – 2011. – № 4. – С. 131-136.
5. Бондарев, П.В. Физическая защита ядерных объектов / П.В. Бондарев, А.В. Измайлов, А.И. Толстой. М.: МИФИ, 2008. – 584 с.
6. Руднев, А.Н. Анализ беспроводных сетей, использующихся при выполнении работ с радиационным фактором / А.Н. Руднев, Р.А. Рязанов // T-Comm: Телекоммуникации и транспорт. – 2011. – № 10. – С. 81-82.
7. Костин, В.Н. Методики, модели и методы обоснования и разработки систем физической защиты критически важных объектов: автореф. дис. на соиск. ученой степ. д-ра техн. наук. / В.Н. Костин Оренбург: Оренбургский гос. ун-т, 2021. – 38 с.
8. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
9. Минпромторг утвердил перечни типовых объектов КИИ в металлургии, горнодобывающей промышленности и ОПК. URL: https://ru-bezh.ru/zakonodatelstvo-i-normativyi/news/24/01/29/minpromtorg-utverdil-perechni-tipovyh-obektov-kii-v-metallurgii (дата обращения: 25.01.2024).
10. Постановление Правительства РФ от 08.02.2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»
11. Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».
12. Приказ ФСТЭК РФ от 25.12.2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
13. Приказ ФСБ России от 19.06.2019 г. № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации».
14. Гавришев, А.А. Анализ технологий защиты радиоканала охранно-пожарных сигнализаций от несанкционированного доступа / А.А. Гавришев, А.П. Жук, Д.Л. Осипов // Труды СПИИРАН. – 2016. – Вып. 4(47). – С. 28-45. DOI: 10.15622/sp.47.2
15. Брауде-Золотарев, Ю. Алгоритмы безопасности радиоканалов / Ю. Брауде-Золотарев // Алгоритм безопасности. – 2013. – № 1. – С. 64-66.
16. Мальцев, Г.Н. Исследование защищенности системы командного радиоуправления подвижным объектом с использованием марковской модели преодоления нарушителем многоуровневой системы защиты информации / Г.Н. Мальцев, С.А. Матвеев // Труды Военно-космической академии имени А.Ф. Можайского. – 2021. – № 677. – С. 153-163.
17. Членов, А.Н. Анализ способов нейтрализации тревожной сигнализации систем охраны категорированных объектов / А.Н. Членов, Н.А. Рябцев, А.Н. Федин // Технологии техносферной безопасности. – 2017. – № 3. – С. 271-279.
18. Гавришев, А.А. Повышение защищенности беспроводных систем безопасности: аналитический обзор публикаций / А.А. Гавришев // Вестник Новосибирского государственного университета. Серия: Информационные технологии. – 2017. – Т. 15. – № 1. – С. 5-14.
19. Рекомендации «Применение оборудования радиоканальных систем передачи извещений (РСПИ)» Р 78.36.048. М.: НИЦ «Охрана», 2015. 182 с.
20. Список технических средств безопасности, удовлетворяющих «Единым требованиям к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнальнопротивоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации». URL: http://nicohrana.ru/237-spisok-tehnicheskih-sredstv-bezopasnosti.html (дата обращения: 01.02.2024).
21. Каталог продукции НПК «Дедал» URL: https://www.dedal.ru/include/catalog.pdf (дата обращения: 01.02.2024).
22. Реализация требований СП484.1311500.2020 (далее СП484) в приборах Астра серии Pro. URL: https://www.tinko.ru/catalog/download.php?file=185600B0DE45090CA6F364035140DDED.pdf&prodid=1798 (дата обращения: 01.02.2024)

23. Гавришев, А.А. Использование широкополосных методов организации радиосвязи DSSS, FHSS и OFDM в радиоканальных системах охранно-пожарной сигнализации, присутствующих на рынке / А.А. Гавришев // Гражданская оборона на страже мира и безопасности: Материалы V Международной научно-практической конференции, посвященной Всемирному дню гражданской обороны. В 4-х частях, Москва, 01 марта 2021 года. Ч. III. М.: АГПС МЧС России, 2021. – С. 24-27.
24. Постановление Правительства РФ от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»
25. Васильев, В.И. Интеллектуальная система обнаружения атак в локальных беспроводных сетях / В.И. Васильев, И.В. Шарабыров // Вестник Уфимского государственного авиационного технического университета. 2015. № 4. С. 95-105.
26. Лесняк, Д.А. Моделирование комплекса средств защиты информации радиоканалов временными раскрашенными сетями Петри / Д.А. Лесняк, С.А. Матвеев // СПбНТОРЭС. – 2020. – № 1(75). – С. 127-130.

References:

1. Stepanova E. Terrorism as a threat to critical infrastructure. *Svobodnaja mysl'* 2010; 4: 35-48 (In Russ.).
2. Lawrence Fennelly Effective Physical Security. 4th Edition. *Butterworth-Heinemann*. 2013:366
3. Kuzmina N.A. Fixing systems and recognition of unauthorized penetration in the protected zone as an element of effective safety of the transport infrastructure object. *T-Comm*. 2018;5:7-52. DOI: 10.24411/2072-8735-2018-10086 (In Russ.).
4. Volhonskij V.V., Krupnov A.G. Features of the development of the structure of threat detection tools for a protected object. *Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki*. 2011; 4: 131-136 (In Russ.).
5. Bondarev P.V., Izmajlov A.V., Tolstoj A.I. Physical protection of nuclear facilities. Moscow: *MIFI Publ*., 2008: 584. (In Russ.).
6. Rudnev A.N., Rjazanov R.A. Analysis of wireless networks used in the performance of work with the radiation factor. *T-Comm*. 2011; 10: 81-82 (In Russ.).
7. Kostin V.N. Methods, models and methods of substantiation and development of physical protection systems for critical facilities: abstract of the dissertation of the Doctor of Technical Sciences. Orenburg: Orenburgskij gos. un-t, 2021:38. (In Russ.).
8. Federal Law No. 187-FZ dated 26.07.2017 «On the Security of the Critical Information Infrastructure of the Russian Federation» (In Russ).
9. Ministry of Industry and Trade has approved lists of typical CII facilities in metallurgy, mining and defense industry. URL: https://ru-bezh.ru/zakonodatelstvo-i-normativyi/news/24/01/29/minpromtorg-utverdil-perechni-tipovyh-obektov-kii-v-metallurgii (date of access: 25.01.2024). (In Russ.)
10. Decree of the Government of the Russian Federation dated 08.02.2018 No. 127 «On Approval of the Rules for Categorizing objects of critical Information Infrastructure of the Russian Federation, as well as a list of indicators of criteria for the significance of objects of critical information infrastructure of the Russian Federation and their values» (In Russ.)
11. Decree of the President of the Russian Federation dated 01.05.2022 No. 250 «On additional measures to ensure information security of the Russian Federation» (In Russ.)
12. FSTEC RF Order No. 239 dated 25.12.2017 «On Approval of Requirements for Ensuring the Security of Significantobjects of the Critical information Infrastructure of the Russian Federation» (In Russ.)
13. Order of the FSB of Russia dated 19.06.2019 No. 282 «On Approval of the Procedure for Informing the FSB of Russia about Computer Incidents, Responding to Them, and Taking Measures to Eliminate the consequences of computer attacks carried out against Significant objects of the Critical Information Infrastructure of the Russian Federation» (In Russ.)
14. Gavrishev A.A., Zhuk A.P., Osipov D.L. Analysis of protection technologies radio fire alarm systems against unauthorized access. *SPIIRAS Proceedings*. 2016;I(4): 28-45. DOI: 10.15622/sp.47.2 (In Russ.).
15. Braude-Zolotarev Yu**.** Safety radio's algorithms. *Algoritm bezopasnosti* . *Safety algorithm*. 2013;1:64-66 (In Russ.).

16. Mal'cev G.N., Matveev S.A. Investigation of the security of the command radio control system of a mobile object using the Markov model of overcoming a multi-level information protection system by an intruder. *Trudy Voenno-kosmicheskoj akademii imeni A.F. Mozhajskogo*. 2021;677:153-163. (In Russ.).
17. Chlenov A.N., Ryabtsev N.A., Fedin A.N**.** Analysis of methods of neutralizing alarm protection systems categorized objects. *Technology of technosphere safety*. 2017; 3: 271-279 (In Russ.).
18. Gavrishev A.A. Analytical Review of Publications Covering the Theme of «Improving the Protection of Wireless Security Systems». *Vestnik NSU. Series: Information Technologies*. 2017; 1: 5-14. (In Russ.).
19. Recommendations «Application of equipment for radio channel notification transmission systems» R 78.36.048. Moscow: *NIC «Ohrana» Publ.*, 2015;182. (In Russ.)
20. The list of technical security equipment that meets the «Uniform requirements for notification transmission systems, object technical security equipment and alarm anti-theft devices of motor vehicles intended for use in non-departmental security units of the National Guard of the Russian Federation». URL: http://nicohrana.ru/237-spisok-tehnicheskih-sredstv-bezopasnosti.html (date of access: 01.02.2024). (In Russ.)
21. Product catalog of NPK «Daedalus». URL: https://www.dedal.ru/include/catalog.pdf (date of access: 01.02.2024). (In Russ.)
22. https://www.tinko.ru/catalog/download.php?file=185600B0DE45090CA6F364035140DDED.pdf&prodid=1798 (date of access: 01.02.2024) Implementation of the requirements of SP484.1311500.2020 (hereinafter SP484) in Astra Pro series devices. (In Russ.)
23. Gavrishev A.A. The use of broadband methods of organizing radio communication DSSS, FHSS and OFDM in radio channel of fire alarm systems present on the market. Civil Defense on guard of peace and security. Proceedings of the V International Scientific and Practical Conference dedicated to the World Civil Defense Day. Vol. III. Moscow: *Academy of the SFS of the Ministry of Emergency Situations of Russia*, 2021; 24-27. (In Russ.).
24. Decree of the Government of the Russian Federation dated 16.04.2012 No. 313 «On Approval of the Regulations on Licensing Activities for the Development, Production, Distribution of Encryption (cryptographic) tools, information systems and Telecommunications Systems Protected using encryption (cryptographic) tools, performance of works, provision of services in the field of information encryption, maintenance of encryption (cryptographic) tools, information systems and telecommunication systems protected using encryption (cryptographic) means (except in the case of, if the maintenance of encryption (cryptographic) means, information systems and telecommunication systems protected using encryption (cryptographic) means is carried out to meet the own needs of a legal entity or an individual entrepreneur)». (In Russ.)
25. Vasilev V.I., Sharabyrov I.V. Intelligent intrusion detection system in local wireless networks. *Vestnik UGATU*. 2015; 4: 95-105 (In Russ.).
26. Lesnyak D.A., Matveev S.A. Modeling of the complex of information protection means of radio channels with temporary colored Petri nets. *SPbNTORES*. 2020;1:127-130 (In Russ.).

Сведения об авторе:
Гавришев Алексей Андреевич, кандидат технических наук, доцент; доцент кафедры стратегические информационные исследования; доцент кафедры международной информационной безопасности; alexxx.2008@inbox.ru
Information about author:
Aleksey A. Gavrishev, Cand. Sci. (Eng.), Assoc. Prof., Assoc. Prof., Department of Strategic Information Research; Assoc. Prof., Department of International Information Security; alexxx.2008@inbox.ru

Конфликт интересов/Conflict of interest.
Автор заявляет об отсутствии конфликта интересов/The author declare no conflict of interest.
Поступила в редакцию/Received 27.09.2024.
Одобрена после/рецензирования Reviced 01.11.2024.
Принята в печать/ Accepted for publication 29.12.2024.