УДК 004.056

***С.П. Серёдкин*[1]**

[1] *Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация*

БЕЗОПАСНОСТЬ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ (КРАТКИЙ ОБЗОР СОВРЕМЕННЫХ ПОДХОДОВ).

Аннотация. В предлагаемой статье рассматриваются основные понятия по обеспечению безопасности критической информационной инфраструктуры (КИИ). Определены основные мероприятия, необходимые для реализации требований федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Представлена тематика вопросов в соответствие с пунктом 1«Безопасность и противодействие терроризму» из перечня приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации» (утверждён Указом Президента Российской Федерации от 7 июля 2011 г. №899). Показан текущий обзор реализации требований по защите информации и анализ кибератак в отношении объектов КИИ. Проанализированы современные подходы к созданию системы безопасности значимых объектов как механизма защиты жизненно важных интересов общества от террористических угроз. Подчеркнута важная роль обеспечения безопасности объектов КИИ как первоочередной задачи для бизнеса и государства.

Ключевые слова: Критическая информационная инфраструктура (КИИ), объекты КИИ, субъекты КИИ, Федеральные органы исполнительной власти (ФОИВ), категорирование объектов информационной инфраструктуры, кибератаки, категории значимости объектов.

***S.P. Seryodkin*[1]**

[1]*Irkutsk State Transport University, Irkutsk, Russian Federation*

AN OVERVIEW OF THE MODERN APPROACH OF SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE

Annotation. The proposed article discusses the basic concepts of ensuring the security of critical information infrastructure. We identified the main measures necessary to implement the requirements of Federal Law No. 187-FL dated 26.07.2017 "On the Security of the Critical Information Infrastructure of the Russian Federation" and presented the current review of the implementation of information protection requirements and the analysis of cyber-attacks against objects of the critical information infrastructure.

Keywords: Critical information infrastructure, objects of the critical information infrastructure, subjects of the critical information infrastructure, Federal Executive Authorities, categorization of information infrastructure objects, cyber-attacks, categories of significance of objects.

Введение. В период возрастающей роли информационных технологий в обеспечении производственно-хозяйственной и финансовых сфер экономики, возрастает число угроз информационной безопасности направленных на объекты информационной инфраструктуры. Позиция государства по данному вопросу определена в Концепции внешней политики Российской Федерации (Указ Президента от 30.11.2016г. №640) и определяет позицию государства в обеспечении необходимых мер для обеспечения национальной и международной безопасности в противодействие угрозам, исходящим из информационного пространства [1].

В Доктрине информационной безопасности Российской Федерации (Указ Президента от 05.12.16г.№646), определены приоритетные цели и задачи обеспечения информационной безопасности. В Концепции к основным национальным интересам в информационной сфере отнесено устойчивое и бесперебойное функционирование в первую очередь критической информационной инфраструктуры [2].

Доказательным примером деструктивного воздействия злоумышленников на КИИ явились масштабные кибератаки в мае-июне 2017 г. программного продукта типа Petya, WannaCry, Misha используя уязвимость EternalBlue [3]. В результате атак было нарушено

штатное функционирование информационных систем (Сбербанка, Пенсионного фонда, ОАО РЖД, ОАО Мегафон). Для скорейшего решения вопросов обеспечения защиты информационно-теле коммутационных сетей и автоматизированных систем управления вводится в действие закон по обеспечению безопасности критической информационной инфраструктуры № 187 ФЗ. Данный закон предъявляет новые требования по обеспечению безопасности объектов информационной инфраструктуры и определяет сферы действия, это: здравоохранение, наука, транспорт, связь, энергетика, атомная промышленность топливо-энергетический комплекс, банки, оборона, ракетно-космическая, горнодобывающая, металлургическая и химической промышленности. Тем самым государство определило принципы, порядок и механизмы обеспечении безопасности КИИ.

Чем вызван тот факт, что государство решило изменить существующий порядок обеспечения защиты информации на объектах информационной инфраструктуры? В своей статье я постараюсь дать необходимую информацию по данному вопросу, а также основные этапы по реализации требований к защите объектов КИИ.

Анализ основных подходов по реализации требований к защите объектов КИИ.

Применяемая ранее терминология в отношении к важным объектам; объект особой важности, критически важный объект, потенциально опасный объект, определяли особый режим требований к защите данных объектов от посягательств злоумышленников, криминальных структур, разведок иностранных государств и т.д.? Защита данной категории объектов обеспечивалась обязательными требования к режиму охраны, системам инженерно-технической и электронной защиты, с целью недопущения негативных воздействий, на население, экологию и окружающую среду в результате вывода из строя производственных объектов с опасными производствами.

Сегодня в результате массовой информатизации экономики и общества, внедрение в производственные процессы автоматизированных систем управления (АСУ), программных продуктов по обеспечению функционирования бизнес-процессов, основанных на передовых информационных технологиях, возросло и количество угроз безопасности информации. В связи с этим фактом доля управления производством и услугами на основе информационных технологий существенно возросла.

События последних 10 лет показывают, что существенно возросло количество кибератак на объекты: финансово банковской сферы, оборонного комплекса, потенциально опасные производства, объекты государственного управления. Все эти факты явились причинами для необходимости изменения подходов к защите данной категории объектов, сделав акцент на защите именно информационной инфраструктуры как основного обеспечивающего процесса.

За последние 15 лет вступили в действия и обеспечили нормативно-правовое обеспечения механизмов защиты информации на объектах ряд законов и Постановлений правительства РФ, Руководящих документов ФСБ, ФСТЭК.

Можно с уверенностью сказать, что пройден очень непростой этап формирования единой государственной политики в области защиты информации. Принятая в 2016г. Доктрина информационной безопасности по сути определила программу действий по защите информации в том числе к критическим важным и потенциально опасным объектам как приоритетную категорию национальных интересов. Государственные регулирующие органы, в свою очередь разработали требования, направленные на повышение безопасности критически важных и потенциально опасных объектов, подтверждение этому принятый в 2017г ФЗ №187.

Для обеспечения исполнения требований ФЗ №187 принимается ряд Указов Президента: № 31с от 15.01.2013, № 569 от 25.11.2017, № 620 от 22.12.2017, № 98 от 02.03. 2018.Внесены изменения в Федеральные законы: № 193-ФЗ от 26.07.2017, № 194-ФЗ от

27.07. 2017г. Приняты Постановления Правительства № 127 от 08.02.2018г, № 162 от 17.02.2018.

В данных документах определены понятия критической информационной инфраструктуры, объектов и субъектов информационного взаимодействия. Определён механизм реализации требований по защите информации, а также определены роли систем государственного контроля и мониторинга за компьютерными инцидентами.

Определены функции ФОИВ в лице ФСБ и ФСТЭК по реализации государственных функций [Рис. 1].

ФСБ России	**ФСТЭК России**
«точка входа» – НКЦКИ, http://gov-cert.ru • нормативно-правовое регулирование в области обеспечения безопасности КИИ • разработка требований к средствам ОПЛ КА • регулирование и координация деятельности субъектов КИИ в части сил и средств ОПЛ КА • сбор информации о компьютерных инцидентах • оценка безопасности КИИ	«точка входа» otd25@fstek.ru • нормативно-правовое регулирование в области обеспечения безопасности КИИ • категорирование объектов КИИ (включая ведение реестра значимых объектов КИИ) • разработка требований по обеспечению информационной безопасности объектов КИИ и государственный контроль в данной области

Рис.1. Функции федеральных органов исполнительной власти.

Создана государственная система обнаружения, предупреждения и ликвидации последствия компьютерных атак на информационные системы РФ - ГосСОПКА.

ГосСОПКА – единый территориально распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. ГосСОПКА обеспечивает через свою инфраструктуру обнаружение компьютерных инцидентов из событий, поступающих от операционных систем, средств обнаружения вторжений, межсетевых экранов, антивирусного программного обеспечения и иных эксплуатируемых средств защиты на объектах КИИ [Рис. 2].

Рис.2. Схема взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствия компьютерных атак на информационные системы РФ - ГосСОПКА.

ФСБ России создан Национальный координационный центр по компьютерным инцидентам (НКЦКИ). (4). НКЦКИ (подразделение ФСБ России) координирует и учувствует в мероприятиях по реагированию на компьютерные инциденты между субъектами КИИ, а

также участвует в процессах обнаружения, предупреждения и ликвидации последствий компьютерных атак на объектах КИИ [Рис. 3].

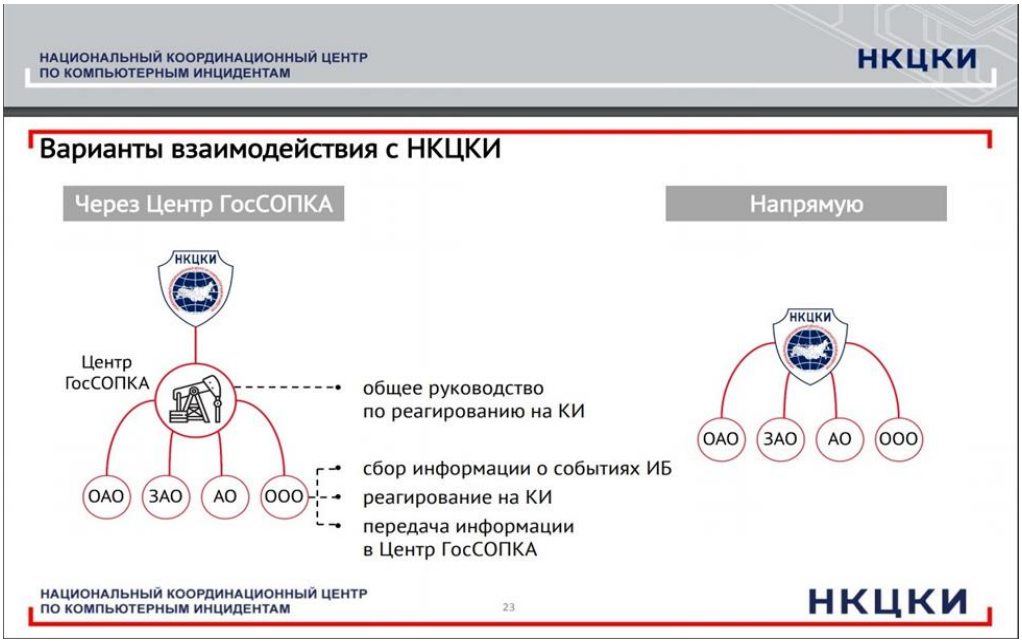

Рис.3. Функции НКЦКИ

Таким образом, НКЦКИ является подразделением ФСБ России и составной частью ГосСОПКА. Согласно Приказу ФСБ России № 366, НКЦКИ осуществляет следующие основные функции:

- Координирует и учувствует в мероприятиях по реагированию;
- Организует и осуществляет обмен информацией о компьютерных инцидентах между субъектами КИИ [4].

Таким образом, государство создает механизм защиты информационных ресурсов объектов КИИ.

Для реализации требований ФЗ№187 определены права и обязанности субъектов критической информационной инфраструктуры, в т.ч обязанности:

1. Категорировать объекты КИИ;
2. Выполнять требования по обеспечению безопасности объектов КИИ (ФСТЭК России);
3. Устанавливать и эксплуатировать средства ОПЛ КА (центры ГосСОПКА и конкретные технические средства – ФСБ России);
4. Реагировать на компьютерные инциденты, информировать о них и принимать меры по ликвидации последствий (ФСБ России);
5. Содействовать должностным лицам ФСБ и ФСТЭК России при исполнении ими своих служебных обязанностей.

Важным этапом реализации требований ФЗ является категорирование объектов информационной инфраструктуры, которую обязан провести субъект (собственник) информационной инфраструктуры. Для этого необходимо провести инвентаризацию информационной инфраструктуры для выявления потенциально значимых объектов КИИ. Данную процедуру необходимо провести в отношении объектов информационной инфраструктуры обеспечивающих управленческие, финансово-экономические, производственные и др. виды деятельности [Рис. 4].

Рис.4. Перечень субъектов и объектов при категорировании

Необходимо оценить масштаб возможных последствий в случае реализации атаки на информационные системы в соответствии с категориями значимости:

- Социальная значимость;
- Политическая значимость;
- Экономическая значимость;
- Экологическая значимость;
- Значимость для обеспечения обороны страны безопасности государства и правопорядка.

В процессе реализации процедуры категорирования проводиться инвентаризация следующих ресурсов:

1.Информационных (базы данных, файлы данных и т.д. с указанием перечня обрабатываемой информации);

2.Программных (системное и прикладное ПО и т.д.);

3.Технических (компьютеры, сервера, коммутационное оборудование, носители данных и т.д.).

Выделить перечень критических процессов предприятия, которые обеспечивают ключевые бизнес-процессы.

Важным элементом категорирования является процедура выявления критичных процессов. Для этого необходимо провести моделирование угроз безопасности в отношении объектов КИИ [Рис. 5].

Оценка угроз безопасности информации проводится в целях определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях с заданной архитектурой и в условиях их функционирования – актуальных угроз безопасности информации [5].

Оценить масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ. в соответствии с перечнем показателей критериев значимости.

После этого необходимо установить по каждому объекту КИИ оду из категорий значимости, либо принять решение об отсутствии необходимости присвоения им категорий значимости. Устанавливается одна из трех категорий, самая высока категория-первая, самая низкая- третья. Перечень объектов КИИ с установленными категориями значимости направляется в ФСТЭК.

После проведения процедуры категорирования объектов КИИ необходимо подготовить план создания системы безопасности объекта КИИ Рис. [6].

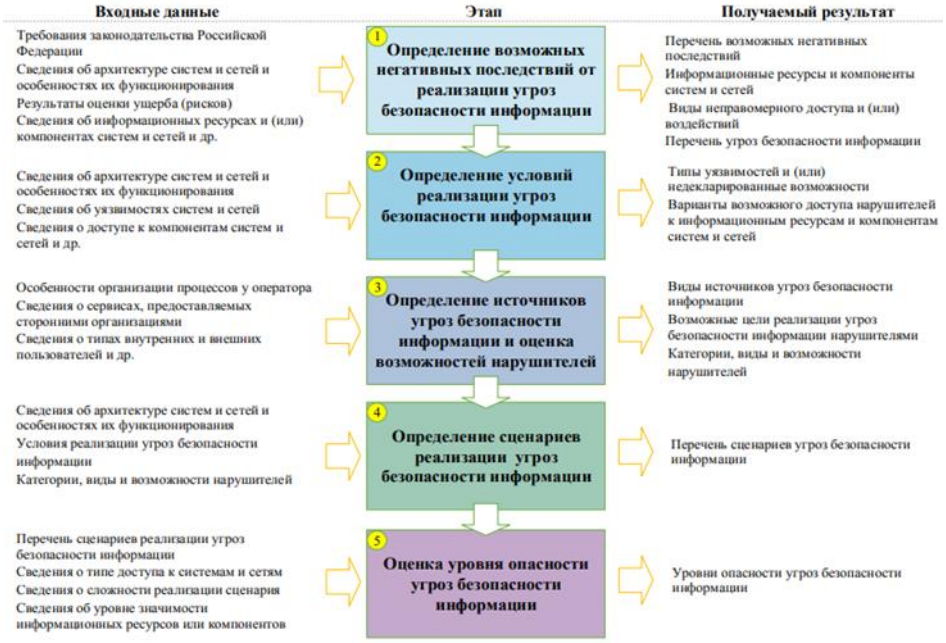

Рис.5. Модель угроз безопасности информации.

Данный этап является самым трудоемким и дорогостоящим процессом и предусматривает разработку:

- организационно-распорядительных документов;
- технического задания на создание системы безопасности;
- технические и организационные мероприятия;
- ввод в действие системы обеспечения безопасности.

Требования, необходимые для обеспечения безопасности объектов КИИ, утверждены приказом ФСТЭК России от 25.12.2017 №239.

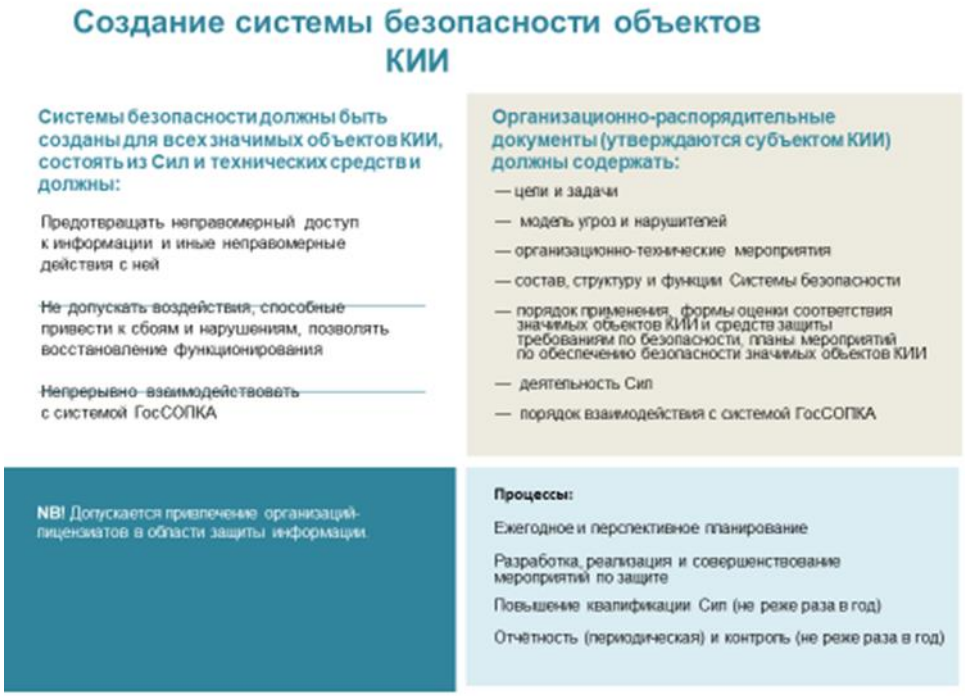

Рис.6. План создания системы безопасности объекта КИИ.

После создания системы обеспечения безопасности субъект организовывает взаимодействие с органами ГосСОПКА. Важно обеспечить функционирование системы

безопасности в актуальном состоянии, производить мониторинг существующей системы защиты, направленной на предотвращение угроз безопасности.

Обзор текущего состояния.

Главным на сегодняшний день является тот факт, что с момента введение в действие ФЗ №187 сделано многое по предотвращению кабератак на информационные ресурсы компаний. Но и сделать предстоит ещё очень многое в вопросах обеспечения безопасности объектов КИИ. Информационный мир изменился, преступные киберсообщества и «одиночки» хорошо подготовленные злоумышленники, имеют на вооружении современные технические средства и оборудование позволяющее преодолевать системы защиты предприятий и учреждений. В сентябре 2021 года стало известно о появлении новой хакерской группировки Chamel Gang, которая инициировала атаки на критическую информационную инфраструктуру, в том числе в России. В российских структурах ТЭК и авиапрома хакерам удалось скомпрометировать серверы. Число кибератак на критическую инфраструктуру РФ увеличилось на 150%. По сравнению с аналогичным периодом прошлого года. Российская компания Group-IB подсчитала, что 40% всех атак совершают «классические» киберпреступники. А вот остальные 60% приходятся на проправительственные агентства других государств. Эксперты прогнозируют, что число кибератак в дальнейшем будем только увеличиваться, а суммы, запрашиваемые мошенниками, будут расти [6].

Выводы. Актуальность информации и выводы, приведенные в статье очевидны, т.к угрозы информационной безопасности на объекты КИИ влекут за собой довольно масштабные последствия не только для бизнеса но и для жизненно важных интересов общества. Несомненно, обеспечение безопасности объектов КИИ первоочередная задача для бизнеса и государства.

Надеемся, что изложенные в статье информация найдет понимание и применение в различных сферах образования и производства для студентов и специалистов по защите информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. «Концепция внешней политики Российской Федерации». Утверждена Указом Президента Российской Федерации от 30 ноября 2016 N 640.
2. «Доктрина информационной безопасности Российской Федерации». Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.
3. Positive Technologies. Вебсайт. Москва, 2002. Режим доступа: https://www.ptsecurity.com.
4. Приказ ФСБ России от 24 июля 2018 г. N 366 "О Национальном координационном центре по компьютерным инцидентам".
5. Методика оценки угроз безопасности: методический документ / сост. ФСТЭК России. – Москва, 2021. – 83 с.
6. Информационно-аналитический журнал «RUБЕЖ» [Электронный ресурс]. – Москва. – 2013 г. – Режим доступа : https://ru-bezh.ru, свободный.
7. «Приоритетные направления развития науки, технологий и техники в Российской Федерации и перечень критических технологий Российской Федерации». Утверждены Указом Президента Российской Федерации от 7 июля 2011 года № 899.
8. Воронов В.А., Тихонов В.А. Концептуальные основы создания и применения системы защиты объектов. – М.: Горячая линия – Телеком, 2013.
9. Федеральный закон от 26 июня 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
10. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
11. Федеральный закон от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

12. Федеральный закон от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации».

13. Указ Президента Российской Федерации от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

14. Указ Президента Российской Федерации от 17 августа 2008 г. № 351 «О мерах по обеспечении информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

15. Защита критически важных объектов инфраструктуры от террористических атак: Сборник передового опыта. [Электронный ресурс]. Режим доступа: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_ru.pdf. свободный.

REFERENCES

1. Foreign Policy Concept of the Russian Federation (approved by President of the Russian Federation Vladimir Putin No. 640 of November 30, 2016).

2. Doctrine of Information Security of the Russian Federation (approved by Decree of the President of the Russian Federation No.646 of December 5, 2016).

3. Positive Technologies. Company website. Moscow, 2002. Access mode: https://www.ptsecurity.com.

4. FSS Order No.366 of July 24, 2018 “On National Computer Incident Response & Coordination Center”.

5. Methodology for assessing security threats: methodological document / comp. FSTEC of Russia. - Moscow, 2021. - 83 p.

6. Information and analytical journal "RUБЕЖ". Electronic resourse. - Moscow, 2013 - Access mode: https://ru-bezh.ru, free.

7. Priority directions for the development of science and technology in the Russian Federation and the list of critical technologies of the Russian Federation (approved by Decree of the President of the Russian Federation No. 899 of July 7, 2001).

8. Voronov V.A., Tikhonov V.A., Conceptual foundations for the creation and application of an object protection system. – M.: Goryachaya linia – Telecom, 2013.

9. On the Security of the Critical Information Infrastructure of the Russian Federation (Federal Law No. 187-FZ of June 26, 2017).

10. On Information, Information Technologies and Information Protection (Federal Law No. 149-FZ of July 27, 2006).

11. On Licensing of Certain Types of Activities (Federal Law No. 99-FZ of May 04, 2011).

12. On Standardization in the Russian Federation (Federal Law No. 162-FZ of June 29, 2015).

13. On improving the State system for detecting, preventing and eliminating the consequences of computer attacks on the Information resources of the Russian Federation (Decree of the President of the Russian Federation No. 620 of December 22, 2017).

14. On measures to ensure information security of the Russian Federation due using information and telecommunication networks of international information exchange (Decree of the President of the Russian Federation No. 351 of August 17, 2008).

15. Protecting critical infrastructure from terrorist attacks. [Access mode: https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_ru.pdf].

Информация об авторе

Серёдкин Сергей Петрович – к. э. н., доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: sseryodkin2008@yandex.ru.

Author

Seryodkin Sergei Petrovich – Ph. D. in Economics, Associate Professor, the Subdepartment of Information systems and information security, Irkutsk State Transport University, Irkutsk, e-mail: sseryodkin2008@yandex.ru.

Для цитирования

Серёдкин С.П. Безопасность критической информационной инфраструктуры, обзор современного подхода. // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. 2021. – №4(12). – С. 30-38 – DOI: 10.26731/2658-3704.2021.4(12).30-38 – Режим доступа: http://ismm-irgups.ru/toma/412-2021, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 27.01.2022)

For citations

Seryodkin S.P. Scientific approaches to the justification of investments in data security // Nauchnye podkhody k obosnovaniyu investiciy v zashity informacii [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2021. No. 4(12). P. 30-38. DOI: 10.26731/2658-3704.2021.4(12).30-38 [Accessed 27/01/22]