БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2022. – № 1 (104). – 27–40

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.9 DOI: 10.17212/2782-2230-2022-1-27-40

АНАЛИЗ МЕТОДИЧЕСКОГО И ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРОЦЕДУР ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА*

Е.Н. ПИВКИН[1], А.А. АРДАЕВА[2]

[1] *105066, РФ, г. Москва, ул. Новорязанская, 31/7, к. 2, ПАО АКБ «Связь-Банк», кандидат технических наук. E-mail: evpiv@yandex.ru*
[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, магистрант кафедры вычислительной техники. E-mail: nastya.ardaeva@yandex.ru*

В настоящей работе проводится непосредственный анализ существующих методик оценивания защищенности значимых объектов критической информационной инфраструктуры, обзор их законодательных основ и существующих средств защиты информации от несанкционированного доступа. Такой анализ необходим для решения задач, связанных с разработкой комплексного подхода к оцениванию защищенности значимых объектов критической информационной инфраструктуры. Рассмотрены основные руководящие документы и приказы ФСТЭК России, Федеральный закон № 187-ФЗ от 26 июля 2017 г. «О безопасности КИИ РФ». Проанализирован современный рынок средств защиты информации от несанкционированного доступа. Для удобства все сравнительные критерии разделены на категории: общие сведения; системные требования (минимальные); поддерживаемые автоиатизированные рабочие места и серверы на основе известных защищенных операционных систем; уровень сертификации по требованиям безопасности ФСТЭК России; развертывание системы защиты; обновление компонентов; основные функции средств защиты информации от несанкционированного доступа; очистка информации; дополнительные модули защиты; централизованное управление и отчетность; возможность интеграции; лицензирование. Для участия в сравнении были выбраны четыре наиболее популярные в России группы средств защиты информации от несанкционированного доступа: Secret Net Studio; Dallas Lock 8.0-K; Diamond ACS; «Блокхост-Сеть 2.0». С целью выявления методик оценивания защищенности значимых объектов критической информационной инфраструктуры рассмотрены национальные стандарты России и

* Статья получена 04 февраля 2022 г.

научная периодика. Показано, что методическое обеспечение данного сегмента безопасности находится не на должном уровне.

Ключевые слова: сравнительный анализ, методики оценивания защищенности, значимые объекты, критическая информационная инфраструктура, информационная безопасность, законодательные основы, средства защиты информации, несанкционированный доступ

ВВЕДЕНИЕ

После вступления в силу Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (КИИ) [1], регулирующего деятельность по обеспечению безопасности объектов информационной инфраструктуры РФ, функционирование которых критически важно для экономики государства, актуальность построения систем защиты информации (СЗИ) на объектах КИИ не вызывает сомнений. Документ определяет описание субъекта и объекта КИИ, безопасности КИИ и компьютерного инцидента. В Постановлении Правительства РФ от 08.02.2018 № 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» [2] определены правила категорирования объектов КИИ. Также принят Приказ ФСТЭК № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ» от 25.12.2017 [3]. Деятельность, относящаяся к обеспечению информационной безопасности (ИБ), должна быть качественно организована и проконтролирована. Для этого необходимо регулярное оценивание уровня защищенности значимых объектов критической информационной инфраструктуры (ЗО КИИ), рисков и мер, принимаемых для управления этими рисками.

Целью настоящей работы является сравнительный анализ методик оценивания защищенности ЗО КИИ от несанкционированного доступа (НСД), их законодательной основы и существующих СЗИ от НСД.

1. АНАЛИЗ НОРМАТИВНО-ПРАВОВЫХ ДОКУМЕНТОВ ПО ОЦЕНИВАНИЮ ЗАЩИЩЕННОСТИ ЗО КИИ

В этом разделе рассмотрим наиболее значимые руководящие документы ФСТЭК России, устанавливающие критерии для оценивания защищенности объектов информатизации.

В Руководящем документе «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации» [4] приводится классификация средств по уровню безопасности от НСД на основе перечня показателей защищенности и совокупности описывающих их требований. Главной основой для разработки данного документа послужила «Оранжевая книга». Этот стандарт устанавливает семь классов защищенности СВТ (средства вычислительной техники) от НСД к информации.

Классы делятся на четыре группы, которые различаются по уровню защиты: в первую группу входит лишь седьмой класс, к которому относят все средства, не соответствующие требованиям более высоких классов; во вторую группу входят шестой и пятый классы, и она характеризуется дискреционной защитой; в третью группу входят четвертый, третий и второй классы, и она характеризуется мандатной защитой; четвертая группа включает в себя лишь первый класс и характеризуется верифицированной защитой. Самый высокий класс – первый, самый низкий – седьмой.

В Руководящем документе «Автоматизированные системы. Защита от НСД к информации [5]. Классификация автоматизированных систем (АС) и требования по защите информации» приведены классификация АС, подлежащих защите от НСД к информации, и требования по защите информации в АС различных классов.

В документе выделяют девять классов защиты АС от НСД к информации. Каждый класс характеризуется определенным минимальным набором требований к безопасности. Классы делятся на три группы, которые различаются по свойствам обработки информации в АС.

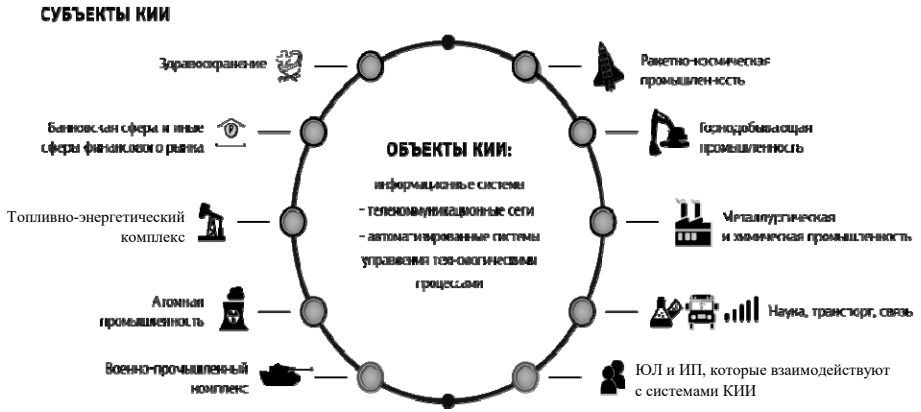
Внутри каждой группы поддерживается иерархия требований безопасности, зависящая от ценности и конфиденциальности информации, и соответственно, иерархия классов защищенности АС.

Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации» [6] является основным для анализа внешней системы защиты периметра корпоративной сети. Этот документ определяет показатели защищенности межсетевых экранов. Каждый критерий защищенности представляет собой набор требований безопасности, характеризующих конкретную область эксплуатации МЭ. В документе описаны пять показателей защищенности.

В данном случае рассматриваются информационные системы (ИС) ЗО КИИ Российской Федерации. При нарушении функционирования предприятия, которое может вызвать сбой ИС, масштаб ущерба крайне сложно определить.

Базовым законом систем ЗО КИИ является Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности КИИ РФ», регулирующий деятельность по обеспечению безопасности объектов информационной инфраструктуры РФ, функционирование которых критически важно для экономики государства. Такие объекты в ФЗ называются объектами КИИ.

Федеральный закон № 187 четко определяет, что «к субъектам критической информационной инфраструктуры относятся государственные органы и учреждения, а также российские юридические лица и/или индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления» [1]. У каждого субъекта КИИ есть объекты КИИ: ИС, АС управления технологическими процессами, информационно-телекоммуникационные сети (рисунок).



Субъекты и объекты критической информационной инфраструктуры

Subjects and objects of critical information infrastructure

В ФЗ № 187 четко регламентированы обязанности субъекта КИИ: категорирование объектов КИИ; выполнение требований по безопасности ЗО КИИ; обеспечение взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА). При рассмотрении систем ЗО КИИ необходимо учитывать не только ФЗ № 187, но и Приказ ФСТЭК России от 25 декабря 2017 г. № 239, в котором обозначены требования по обеспечению безопасности на всех стадиях

жизненного цикла, а также требования по внедрению организационных и технических мер по обеспечению безопасности ЗО КИИ. В 2019 г. были внесены поправки в приказы ФСТЭК России № 239 [3] и № 17 [7], что ознаменовало переход к новой системе требований, предъявляемых к средствам защиты информации.

В настоящее время система требований к оцениванию основывается на уровнях доверия, устанавливаемых приказом ФСТЭК России № 131 [8]. Дополнительно к нему вышла методика выявления уязвимостей и недекларированных возможностей в программном обеспечении. Выполнение требований к уровню доверия является обязательным при проведении работ по оцениванию соответствия, в том числе и в форме сертификации СЗИ, организуемых ФСТЭК России в пределах своих полномочий. Требования к разработке и производству СЗИ, к проведению испытаний СЗИ, а также к поддержке безопасности СЗИ в ходе их применения устанавливаются требованиями к уровням доверия. Для дифференциации указанных требований устанавливается шесть уровней доверия. Самый низкий уровень – шестой, самый высокий – первый [9].

2. АНАЛИЗ СРЕДСТВ ЗАЩИТЫ ОТ НСД ДЛЯ ЗО КИИ

Для удобства анализа современных СЗИ все сравнительные критерии были разделены на следующие категории: общие сведения; системные требования (минимальные); поддерживаемые автоматизированные рабочие места (АРМ) и серверы на основе известных защищенных операционных систем; уровень сертификации по требованиям безопасности ФСТЭК России; развертывание системы защиты; обновление компонентов; основные функции СЗИ от НСД; очистка информации; дополнительные модули защиты; централизованное управление и отчетность; возможность интеграции; лицензирование.

Для участия в сравнении были выбраны четыре наиболее популярные в России СЗИ от НСД: Secret Net Studio; Dallas Lock 8.0-K; Diamond ACS; «Блокхост-Сеть 2.0».

Исходя из анализа средств защиты информации от несанкционированного доступа, можно сделать вывод о том, что комплекс хорошо описанных организационных процессов и общей архитектуры системы защиты имеет гораздо большее значение, нежели отдельные внедряемые механизмы безопасности (таблица).

Сравнение СЗИ от НСД

Comparison of SPI from NSD

Параметр сравнения	Secret Net Studio	Dallas Lock	Diamond ACS	Блокхост-Сеть
Компания-вендор	ООО «Код Безопасности»	ООО «Конфидент»	ООО «ТСС»	ООО «Газинформсервис
Целевой сегмент	Крупный бизнес, средний бизнес. Государственный сектор			
Интерфейс	Русский, английский	Русский	Русский, английский	Русский, английский
Требования к серверу безопасности системы	CPU Intel Core i5/Intel Xeon E3, RAM 8 GB, HDD 150 GB	Конфигурация сервера определяется требованиями к соответствующей ОС. Для размещения файлов СЗИ НСД требуется не менее 200 MB HDD	Конфигурация сервера определяется требованиями к соответствующей ОС	Конфигурация сервера определяется требованиями к соответствующей ОС из списка разрешенных к применению
Поддерживаемые операционные системы	Windows Server 2008 R2, Windows Server 2012/2012R2, Windows Server 2016, windows Vista, Windows 7, Windows 8/8.1, Windows 10			
Уровень сертификации по требованиям безопасности ФСТЭК России	РД СВТ – 5-й класс защищенности СВТ от НСД	РД СВТ – 5-й класс защищенности СВТ от НСД	РД СВТ – 3-й класс защищенности СВТ от НСД	РД СВТ – 5-й класс защищенности СВТ от НСД

Продолжение таблицы

Table continuation

Параметр сравнения	Secret Net Studio	Dallas Lock	Diamond ACS	Блокхост-Сеть
	РД НДВ – 4-й уровень контроля отсутствия НДВ МЭ – 4-й класс защиты МЭ СКН – 4-й класс защиты СКН САВЗ – 4-й класс защиты САВЗ СОВ – 4-й класс защиты СОВ	РД НДВ – 4-й уровень контроля отсутствия НДВ МЭ – нет СКН – 4-й класс защиты СКН САВЗ – нет СОВ – 4-й класс защиты СОВ	РД НДВ – 2-й уровень контроля отсутствия НДВ МЭ – нет СКН – нет САВЗ – нет СОВ – нет	РД НДВ – 4-й уровень контроля отсутствия НДВ МЭ – класс защиты МЭ СКН – 4-й класс защиты СКН САВЗ – нет СОВ – нет
Параметр сравнения	Secret Net Studio	Dallas Lock	Diamond ACS	Блокхост-Сеть
Контроль входа в систему, блокировка сеанса работы	Да	Да	Да	Да
Контроль объектов системы	Да	Да	Да	Да
Контроль целостности системы	Да	Да	Нет	Нет
Контроль портов ввода/вывода подключаемых устройств	Да	Да	Да	Да
Персональный межсетевой экран	Да	Да	Нет	Да

Окончание таблицы

End of Table

Параметр сравнения	Secret Net Studio	Dallas Lock	Diamond ACS	Блокхост-Сеть
Средство обнаружения вторжения уровня хоста	Да	Да	Нет	Нет
Средство антивирусной защиты	Да	Нет	Нет	Нет
Управление и мониторинг СЗИ	Да	Да	Да (для автономной версии)	Да
Регистрация и учет событий	Да	Да	Да	Да
Описание политики лицензирования	По числу защищаемых компьютеров / по защитным модулям	По числу защищаемых компьютеров / по защитным модулям	По числу рабочих мест. Лицензия на использование сервера управления приобретается отдельно	По числу рабочих мест. Лицензия на использование сервера управления приобретается отдельно

3. АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДИК ОЦЕНИВАНИЯ ЗАЩИЩЕННОСТИ ОТ НСД ДЛЯ ЗО КИИ

Разработку методических рекомендаций по оцениванию защищенности объектов информатизации и изменению структуры системы ее защиты проводили, например, Л.Г. Осовецкий и С.В. Максименко применительно к АС обработки данных, однако систему в целом для ЗО КИИ не рассматривали, для оценивания вероятности конкретной угрозы использовали экспертные оценки.

В Приказе ФСТЭК России № 131 отражены в основном требования к защите ЗО КИИ, но пользователям не предоставляются ни методология оцени-

вания эффективности, ни требования к разработке, оформлению и содержанию необходимых документов.

ГОСТ Р ИСО/МЭК ТО 19791–2008 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» [10] содержит рекомендации и критерии оценивания безопасности АС, а также обеспечивает расширение области применения стандартов серии ИСО/МЭК 15408, включая ряд критических аспектов, касающихся оценивания среды эксплуатации объекта, оценивания и декомпозиции составных АС на домены безопасности, которые должны оцениваться отдельно. Устанавливает определение и модель АС; описывает расширения концепции оценивания безопасности с помощью стандартов серии ИСО/МЭК 15408; методологию и процесс выполнения оценивания безопасности АС; дополнительные критерии оценивания безопасности, охватывающие те аспекты АС, которые не были охвачены критериями оценивания безопасности в стандартах серии ИСО/МЭК 15408. Дает возможность включать продукты безопасности, оцененные в соответствии с требованиями стандартов серии ИСО/МЭК 15408, в автоматизированные системы и проводить оценку как единого целого с использованием настоящего стандарта.

Исходя из анализа национального стандарта РФ ГОСТ Р ИСО/МЭК 15408-1–2012 [11], примерами объекта оценивания являются прикладная программа; операционная система; прикладная программа в сочетании с операционной системой; прикладная программа в сочетании с операционной системой и рабочей станцией; операционная система в сочетании с рабочей станцией; интегральная схема смарт-карты; локальная вычислительная сеть, включая все терминалы, серверы, сетевое оборудование и программные средства; приложение базы данных, за исключением программных средств удаленного клиента, обычно ассоциируемых с приложением базы данных.

В публикациях [12–25] приведены алгоритмы и модели оценивания защищенности некоторых объектов территориальных налоговых органов (ТНО) Российской Федерации (РФ). Авторы приведенных работ не сформулировали методики оценивания защищенности ТНО РФ, это в особенности касается ЗО КИИ, проблематика которых возникла в результате вступления в силу Федерального закона № 187. С учетом существующих разработок для ТНО РФ работы [12–25], на наш взгляд, представляют интерес для дальнейшего развития в рамках модификации и апробации для ЗО КИИ, учитывая, что методические разработки в этом направлении отсутствуют.

ЗАКЛЮЧЕНИЕ

Таким образом, федеральные органы исполнительной власти, которые отвечают за обеспечение ИБ КИИ, действуют на основании своих нормативных документов, в которых отсутствуют описание единого регламента проведения аудита ЗО КИИ и оценочные показатели соответствия требованиям ИБ.

В области ИБ нет национального стандарта, устанавливающего единые регламенты и процедуры проведения аудита, тем более для аудита КИИ (методики, описывающие порядок действий по определению уровня защищенности ОИ, показатели ИБ, способы оценивания показателей и уровней защищенности), общей методики проведения оценивания защищенности объектов информатизации, в том числе и ЗО КИИ, автоматизированных методик даже в рамках экспертного подхода.

БЛАГОДАРНОСТИ

Автор выражает глубокую благодарность д-ру техн. наук, профессору Белову Виктору Матвеевичу за ценные советы и замечания, высказанные при работе над статьей.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Постановление Правительства Российской Федерации «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» от 08.02.2018 № 127 (с изм. и доп. в ред. от 13 апреля 2019 г.).

3. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. Приказов ФСТЭК России от 9 августа 2018 г. № 138, от 26 марта 2019 г. № 60, от 20 февраля 2020 г. № 35).

4. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»: утв. решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

5. Руководящий документ «Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации»: утв. решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

6. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

7. Приказ ФСТЭК России от 21.09.2016 № 131 «Об организации работы по разработке перечней правовых актов и их отдельных частей (положений), содержащих обязательные требования, соблюдение которых оценивается при проведении мероприятий по контролю в рамках видов федерального государственного контроля в сфере компетенции ФСТЭК России».

8. Информационное сообщение «О требованиях безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» от 29.03.2019 № 240/24/1525.

9. ГОСТ Р ИСО/МЭК ТО 19791–2008. Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем: введ. 2009–10–01. – М.: Стандартинформ, 2010. – 121 с.

10. ГОСТ Р ИСО/МЭК 15408-1–2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель: взамен ГОСТ Р ИСО/МЭК 15408-1–2008: введ. 2013–12–01. – М.: Стандартинформ, 2010. – 51 с.

11. *Пивкин Е.Н., Белов В.М.* Нечеткие модели в системе защиты информации, составляющей налоговую тайну // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2008. – № 2 (18), ч. 1. – С. 125–128.

12. *Белов В.М., Пивкин Е.Н., Прокопец В.Д.* Оценка уровня информационной безопасности на основе нечетких моделей в территориальных налоговых органах // Научно-технические ведомости СПбГПУ. – 2007. – № 4-2 (52). – С. 130–132.

13. *Шуроватов М.А., Пивкин Е.Н., Белов В.М.* Программное обеспечение оценки уровня защищенности виртуального канала // Ползуновский альманах. – 2008. – № 4. – С. 90–93.

14. *Капустин А.В., Пивкин Е.Н., Белов В.М.* Программное обеспечение оценки защищенности объектов информатизации на основе аппарата нечетких множеств и стандарта Банка России // Ползуновский альманах. – 2008. – № 4. – С. 97–100.

Пивкин Евгений Николаевич, кандидат технических наук, руководитель направления отдела защиты информации департамента безопасности ПАО АКБ «Связь-Банк». Основное направление научных исследований – применение математических методов в различных областях науки, техники, общества. Автор более 80 публикаций. E-mail*:* evpiv@yandex.ru

Ардаева Анастасия Андреевна, магистрант кафедры вычислительной техники Новосибирского государственного технического университета. Область научных интересов – прикладная информатика, информационная безопасность. E-mail: nastya.ardaeva@yandex.ru

DOI: 10.17212/2782-2230-2022-1-27-40

Analysis of methodological and technical support of procedures for assessing the security of significant objects of critical information infrastructure from unauthorized access*

E.N. Pivkin[1], A.A. Ardaeva[2]

[1] *PJSC JSCB "Svyaz-Bank", 31/7 Street Novoryazanskaya, Moscow, 105066, Russian Federation, candidate of technical sciences, E-mail: evpiv@yandex.ru*
[2] *Novosibirsk State Technical University, Karl Marx Avenue, 20, Novosibirsk, 1630073, Russian Federation, Master's student of the Department of Computer Science. E-mail: nastya.ardaeva@yandex.ru*

This paper provides a direct analysis of existing methods for assessing the security of significant objects of critical information infrastructure, a review of their legislative framework and existing means of protecting information from unauthorized access. Such an analysis is necessary to solve problems related to the development of an integrated approach to assessing the security of significant objects of critical information infrastructure. The main guiding documents and orders of the FSTEC of Russia, Federal Law No. 187-FZ of July 26, 2017 "On the security of the CII of the Russian Federation" were considered. The modern market of means of protecting information from unauthorized access was analyzed. For convenience, all comparative criteria were divided into categories: general information; system requirements (minimum); supported automated workstations and servers based on well-known secure operating systems; the level of certification according to the safety requirements of the FSTEC of Russia; deployment of a protection system; component updates; the main functions of the means of protecting information from unauthorized access; clearing information; additional protection modules; centralized management and reporting; possibility of integration; licensing. The four most popular Russian groups of means of protecting information from unauthorized access were selected to participate in the comparison: Secret Net Studio; Dallas Lock 8.0-K; Diamond ACS; Blockhost Network 2.0. In order to identify methods for assessing the security of significant objects of critical information infrastructure, national standards of Russia and

* *Received 04 February 2022.*

scientific periodicals were considered. It is shown that the methodological support of this segment of safety is not at the proper level.

Keywords: comparative analysis, security assessment methods, significant objects, critical information infrastructure, information security, legal framework, information security tools, unauthorized access

REFERENCES

1. RF Federal Law “On the security of the critical information infrastructure of the Russian Federation” of July 26, 2017 N 187. (In Russian).

2. Decree of the Government of Russia N 127 of February 8, 2018 “On approval of the rules for categorizing the objects of critical information infrastructure of the Russian Federation, and also the list of indicators of the criteria of significance of the objects of critical information infrastructure of the Russian Federation and their values” (as amended on April 13, 2019). (In Russian).

3. Order of the FSTEC of Russia of December 25, 2017 N 239 “On approval of the requirements for ensuring the security of significant objects of critical information infrastructure of the Russian Federation” (as amended by the Orders of the FSTEC of Russia of August 9, 2018 N 138, of March 26, 2019 N 60, of February 20, 2020 N 35). (In Russian).

4. Guidance Document “Computer facilities. Protection against unauthorized access to information. Indicators of security against unauthorized access to information”. Approved by the decision of the State Technical Commission under the President of the Russian Federation of March 30, 1992. (In Russian).

5. Guidance Document “Automated systems. Protection from unauthorized access to information. Classification of automated systems and information security requirements”. Approved by the decision of the State Technical Commission under the President of the Russian Federation of March 30, 1992. (In Russian).

6. Order of the FSTEC of Russia of February 11, 2013 N 17 “On approval of requirements for the protection of information not constituting a state secret contained in state information systems”. (In Russian).

7. Order of the FSTEC of Russia of September 21, 2016 N 131 “On the organization of work on the development of lists of legal acts and their separate parts (provisions) containing mandatory requirements, compliance with which is assessed when carrying out control measures within the framework of types of federal state control within the competence of the FSTEC of Russia”. (In Russian).

8. Information message “On information security requirements that establish levels of trust in technical information security tools and information technology security tools” of March 29, 2019 N 240/24/1525. (In Russian).

9. State Standard R ISO/IEC TO 19791–2008. *Information technology. Security techniques. Security assessment of operational systems*. Moscow, Standartinform Publ., 2010. 121 p. (In Russian).

10. State Standard R ISO/IEC 15408-1–2012. *Information technology. Security techniques. Evaluation criteria for IT security*. Pt. 1. *Introduction and general model*. Moscow, Standartinform Publ., 2010. 51 p. (In Russian).

11. Pivkin E.N., Belov V.M. Nechetkie modeli v sisteme zashchity informatsii, sostavlyayushchei nalogovuyu tainu [Fuzzy models in system of protection of the information containing tax secret]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki = Proceedings of TUSUR University*, 2008, no. 2 (18), pt. 1, pp. 125–128.

12. Belov V.M., Pivkin E.N., Prokopets V.D. Otsenka urovnya informatsionnoi bezopasnosti na osnove nechetkikh modelei v territorial'nykh nalogovykh organakh [Assessment of the level of information security based on fuzzy models in the territorial tax authorities]. *Nauchno-tekhnicheskie vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo universiteta = St. Petersburg State Polytechnical University Journal*, 2007, no. 4-2 (52), pp. 130–132.

13. Shurovatov M.A., Pivkin E.N., Belov V.M. Programmnoe obespechenie otsenki urovnya zashchishchennosti virtual'nogo kanala [Virtual channel security level assessment software]. *Polzunovskii al'manakh = Polzunov Almanac*, 2008, no. 4, pp. 90–93.

14. Kapustin A.V., Pivkin E.N., Belov V.M. Programmnoe obespechenie otsenki zashchishchennosti ob"ektov informatizatsii na osnove apparata nechetkikh mnozhestv i standarta Banka Rossii [Software for assessing the security of informatization objects based on the apparatus of fuzzy sets and the standard of the Bank of Russia]. *Polzunovskii al'manakh = Polzunov Almanac*, 2008, no. 4, pp. 97–100.

Для цитирования:

Пивкин Е.Н., Ардаева А.А. Анализ методического и технического обеспечения процедур оценивания защищенности значимых объектов критической информационной инфраструктуры от несанкционированного доступа // Безопасность цифровых технологий. – 2022. – № 1 (104). – С. 27–40. – DOI: 10.17212/2782-2230-2022-1-27-40.

For citation:

Pivkin E.N., Ardaeva A.A. Analiz metodicheskogo i tekhnicheskogo obespecheniya protsedur otsenivaniya zashchishchennosti znachimykh ob"ektov kriticheskoi informatsionnoi infrastruktury ot nesanktsionirovannogo dostupa [Analysis of methodological and technical support of procedures for assessing the security of significant objects of critical information infrastructure from unauthorized access]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2022, no. 1 (104), pp. 27–40. DOI: 10.17212/2782-2230-2022-1-27-40.