УДК 004.054.53
DOI: 10.33764/2618-981X-2020-6-1-22-30

РАЗРАБОТКА МЕТОДИКИ АУДИТА КИБЕРБЕЗОПАСНОСТИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ, ОТНОСЯЩИХСЯ К ЗНАЧИМЫМ ОБЪЕКТАМ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ, ФУНКЦИОНИРУЮЩИХ НА БАЗЕ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

Владимир Робертович Ан
Новосибирский государственный технический университет, 630073, Россия, г. Новосибирск, пр. Карла Маркса, 20, магистрант кафедры вычислительной техники, тел. (903)939-53-58, e- mail: vovan2011nsk@mail.ru

Валерия Александровна Табакаева
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры фотоники и приборостроения, тел. (962)831-22-52, e-mail: tabakaeva1997@mail.ru

Валентин Валерьевич Селифанов
Новосибирский государственный технический университет, 630073, Россия, г. Новосибирск, пр. Карла Маркса, 20, старший преподаватель кафедры защиты информации тел. (923)247-25-81, e-mail: sfo1@mail.ru

В данной статье рассматривается проблема разработки методики аудита кибербезопасности государственных информационных систем, относящихся к значимым объектам (ЗО) критической информационной инфраструктуры (КИИ), функционирующих на базе центров обработки данных. По требованиям законодательства, государственный контроль проводится в соответствии с Приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Требования. О защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

На данный момент существует множество международных и отечественных рекомендаций и практик по проведению аудита кибербезопасности информационных систем, но они не соответствуют существующим и вновь появляющимся требованиям в сфере обеспечения кибербезопасности ЗО КИИ Российской Федерации и не могут применяться без существенной доработки. Авторы рассматривают задачи, которые необходимо решить для разработки методики аудита, проводят анализ существующих законодательных, нормативных правовых актов Российской Федерации и уполномоченных в данной области федеральных органов исполнительной власти, методических документов и стандартов, а также возможных причин существующей ситуации. В результате исследования предложен алгоритм возможных действий при проведении аудита кибербезопасности в ходе государственного контроля, полученный в результате компиляции международных практик (стандартов) и требований, принятых в Российской Федерации, а также требования к необходимому инструментарию – системам анализа уязвимостей и вспомогательному программному обеспечению (системам управления базами данных).

Ключевые слова: информационная безопасность, кибербезопасность, критическая информационная инфраструктура, государственная информационная система, межведомственный контроль, методика аудита кибербезопасности, оценка существующих методов аудита кибербезопасности.

DEVELOPMENT OF CYBERSECURITY AUDIT METHODOLOGY FOR STATE INFORMATION SYSTEMS RELATED TO SIGNIFICANT OBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE OPERATING ON THE BASIS OF DATA CENTERS

Vladimir R. An
Novosibirsk State Technical University, 20, K. Marx Prospekt, Novosibirsk, 630073, Russia, Graduate, Department of Computer Science, phone: (903)939-53-58, e-mail: vovan2011nsk@mail.ru

Valeria A. Tabakaeva
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Photonics and Device Engineering, phone: (962)831-22-52, e-mail: tabakaeva1997@mail.ru

Valentin V. Selifanov
Novosibirsk State Technical University, 20, K. Marx Prospekt, Novosibirsk, 630073, Russia, Senior Lecturer, Department of Information Security, phone: (923)247-25-81, e-mail: sfo1@mail.ru

The problem of developing a cybersecurity audit methodology for state information systems related to significant objects (SO) of critical information infrastructure (CII), operating on the basis of data centers is considered. In accordance with the requirements of the legislation, state control is carried out in accordance with the Order of the FSTEC of Russia dated February 11, 2013 №17 "Requirements. Ensuring the protection of information not constituting a state secret."

Currently, there are many international and domestic recommendations and practices to conducting cybersecurity audit of information systems, but they do not meet the existing and emerging requirements in the field of cybersecurity of SO CII of the Russian Federation and cannot be applied without significant improvement. The authors consider the issues that need to be solved in order to develop an audit methodology, analyze existing legislative and regulatory acts of the Russian Federation and Federal Executive bodies authorized in this area, methodological documents (MD) and standards, as well as possible reasons for the current situation. An algorithm of possible actions for conducting a cybersecurity audit in the course of state control is proposed. The algorithm is a result of compiling international practices (standards) and requirements adopted in the Russian Federation, as well as requirements to the necessary tools – vulnerability analysis systems and support software (database management systems).

Key words: information security, cybersecurity, critical information infrastructure, state information system, interagency monitoring, cybersecurity audit methodology, assessment of existing methods of cybersecurity audit.

Введение

Из-за необходимости обработки огромных объемов информации с целью реализации полномочий государственных органов, разрабатываются, создаются и внедряются государственные информационные системы(ГИС), которым впоследствии присваивается статус ЗО КИИ. Это вызвано тем, что замедление или прекращение деятельности органов государственной власти может привести к социальному, политическому, экономическому либо экологическому кризису [1].

При рассмотрении Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» более детально, можно констатировать факт, что аудит является обязательным и одним из ключевых моментов на этапах создания и в ходе эксплуатации систем кибербезопасности ЗО КИИ.

Актуальность темы исследования обусловлена необходимостью обеспечения информационной безопасности (ИБ) ГИС, относящихся к ЗО КИИ, функционирующих на базе центров обработки данных(ЦОД), с помощью которых осуществляют поддержку жизнеобеспечения граждан Российской Федерации. В современных условиях, когда ГИС проникают во все сферы деятельности системы государственной власти и органов местного самоуправления, их взаимодействие с сетью Интернет оказывает негативное влияние с точки зрения ИБ, так как они становятся открытыми для реализации угроз внутренними и внешними нарушителями разного потенциала.

Проблема ИБ становится не менее важной, чем экономическая или физическая безопасность. Несмотря на важность рассматриваемой проблемы, в настоящее время не уделяется достаточного внимания выполнению работ, связанных с аудитом кибербезопасности ГИС региональных органов исполнительной власти и органов местного самоуправления. Это связано, прежде всего, с отсутствием необходимой нормативно-правовой базы и методик, неподготовленностью специалистов и недостаточным практическим опытом в области проведения аудита кибербезопасности.

Аудит кибербезопасности является одной из важнейших составляющих для решения данной проблемы.

Аудит кибербезопасности – это форма государственного (межведомственного) контроля, которая включает анализ рисков, связанных с возможностью осуществления угроз безопасности, особенно в отношении информационных ресурсов, оценку текущего уровня защищенности ГИС, оценку соответствия ГИС требованиям нормативно-правовых документов и существующим стандартам в области ИБ и выработку рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ГИС.

В результате аудита кибербезопасности ожидается проведение оценки уровня безопасности ГИС, для поддержания непрерывности бизнес-процессов в целом с учетом перспектив развития этой системы. В данной статье понятия «защита информации», «информационная безопасность» и «кибербезопасность» считаются тождественными.

Методы и методики

Основной особенностью исследуемого аудита кибербезопасности является включение его в состав процедуры государственного контроля, что накладывает на него жесткие требования по неукоснительному соблюдению всех положений следующих видов документов:

1) законодательных актов РФ;

2) нормативных правовых актов РФ и федеральных органов государственной власти;

3) методических документов (МД);

4) международных и национальных стандартов, признанных обязательными в данной сфере.

Помимо этого, необходимо уточнить требования к инструментарию, применяемому при проведении аудита [2]. Не исключая применения сертифицированных систем анализа защищенности (уязвимостей), необходимо использовать дополнительное программное обеспечение (ПО), позволяющее интерпретировать результаты с высокой достоверностью и оперативностью [3].

В действительности такое ПО будет представлять собой базу данных, содержащую следующую информацию:

1) данные по существующим уязвимостям в форме и объеме, позволяющие максимально быстро их интерпретировать, вне зависимости от применяемых сканеров уязвимостей;

2) результаты оценки уровня уязвимости и актуальности возможных угроз безопасности с учетом особенности каждого проверяемого объекта;

3) отчет, полученный в результате сравнения оценок контроля на других подобных объектах.

Для решения проблемы, описанной в данной статье, необходимо разработать и апробировать методику аудита кибербезопасности ГИС, относящихся к ЗО КИИ, функционирующим на базе ЦОД.

Для реализации цели необходимо решить следующие задачи:

1) провести анализ требований к системе кибербезопасности ГИС относящихся к ЗО КИИ, функционирующих на базе ЦОД [4];

2) провести анализ существующего нормативно-методического аппарата аудита кибербезопасности ГИС;

3) разработать методику аудита кибербезопасности;

4) провести ее апробацию.

В данной статье объектом исследования являются системы кибербезопасности ГИС, относящиеся к ЗО КИИ, функционирующие на базе ЦОД. А предметом исследования – процесс проведения аудита кибербезопасности ГИС, относящихся к ЗО КИИ, функционирующим на базе ЦОД.

В ходе анализа существующего нормативно-методического аппарата аудита кибербезопасности ГИС использовалась научная электронная библиотека «elibrary.ru».

Статистика поисковых слов/фраз и количество найденных публикаций представлены в табл. 1.

Таблица 1

Статистика поисковых слов/фраз и количество найденных публикаций

Поисковое слово/фраза	Количество найденных публикаций
Аудит ИБ	498
Аудит кибербезопасности	15
Аудит информационных систем	761

Среди найденных публикаций были выбраны актуальные – опубликованные за последние 5 лет в открытом доступе и наиболее соответствующие объекту и предмету исследования.

В результате анализа публикаций по тематике аудита было выявлено несколько направлений. Одно из направлений – это методики на базе международного стандарта COBIT 5.

В данном направлении авторы рассматривают критерии проведения аудита ИБ с использованием стандарта COBIT. Особое внимание авторы уделяют организационным мероприятиям, направленным на обеспечение защищенности информации, в качестве примера приводят проверку на соответствие регламентов, касающихся установки сложностей паролей, и действительности, а также уровню подготовки специалистов, осуществляющих защиту информации (ЗИ) [5, 6].

Но наиболее популярны методики, основанные на серии стандартов ГОСТ Р ИСО/МЭК 27000. В данном направлении, в основном, авторы предлагают проводить аудит в соответствии с рекомендациями международного стандарта, в частности, можно привести перечень субъективных рекомендаций авторов, содержащий следующее:

– разработка стратегии управления рисками различных классов объектов информатизации [7];

– определение объектов, с которых может производиться съем информации с целью применения мер по снижению рисков до приемлемого уровня [8];

– внедрение внутренних регламентов в области ИБ [9];

– проверка применяемых мер и средств ЗИ от несанкционированного доступа (НСД) с учетом категории объекта [10];

– использование сервисов для повышения осведомленности персонала о кибербезопасности [11];

– увеличение бюджета на обеспечение кибербезопасности [12];

– применение широкого спектра различных сканеров (сканеры безопасности, сканеры уязвимостей, сетевые сканеры) [13];

– применение экспертных систем на основе нечетких множеств с использованием базы знаний, включающих соответствующие требования/рекомендации [14].

Таким образом, если рассматривать существующие методы, основанные на базе серии стандартов ГОСТ Р ИСО/МЭК 27000, то в общем случае аудит ИБ включает в себя:

– проведение оценки рисков, связанных с вероятностью реализации угроз безопасности в отношении активов;

– оценку текущего состояния защищенности информационной системы(ИС);

– оценку соответствия ИС существующим стандартам в области ИБ;

– выработку рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС;

– получение максимальной отдачи от средств, инвестируемых в создание (совершенствование, модернизацию) комплексной системы ИБ.

Аудит ИБ можно разделить на следующие категории:

– экспертный аудит безопасности, в ходе которого выявляются уязвимости в системе мер ЗИ на основе опыта экспертов, участвующих в процедуре обследования;

– оценка соответствия рекомендациям нормативных правовых документов (международным и российским стандартам и др.);

– инструментальный анализ состояния защищенности ИС, направленный на выявление и устранение уязвимостей программно-аппаратного обеспечения системы;

– комплексный аудит, включающий в себя все вышеперечисленные формы проведения обследования.

Результаты

Подводя итог, можно сделать следующий вывод: существующие известные методы проведения аудита универсальны для каждой отдельной организации, с их ИС, учитывающие специфичность их деятельности, но не в отношение ЗО КИИ ГИС, функционирующих на базе ЦОД. Соответственно, не учитываются требования законодательных и нормативно-правовых актов, МД по ЗИ.

В данной работе в качестве основополагающих документов рассматриваются следующие:

– Федеральный закон №187 ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [15];

– Приказ ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» с редакцией от 28 мая 2019 года [16];

– Приказ ФСТЭК России от 21 декабря 2017 г. №235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» [17];

– Приказ ФСТЭК России от 25 декабря 2017 г. №239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [18];

– МД. Меры защиты в ГИС [19];

– МД. Методика выявления уязвимостей и недекларированных возможностей в ПО [20].

На основе проведенного анализа становится ясно, что проведение аудита кибербезопасности предполагает алгоритм действий, включающий в себя множество компонентов, в том числе регулирующих нормативно-правовых требований, которые представлены на схеме проведения аудита (рис. 1).

В результате выполнения поставленной цели и задач будут разработаны:

– методика аудита кибербезопасности ГИС, относящихся к ЗО КИИ, функционирующих на базе ЦОД;

– критерии, используемые при проведении аудита кибербезопасности, на основе которых будет оцениваться защищенность свойств ИБ.

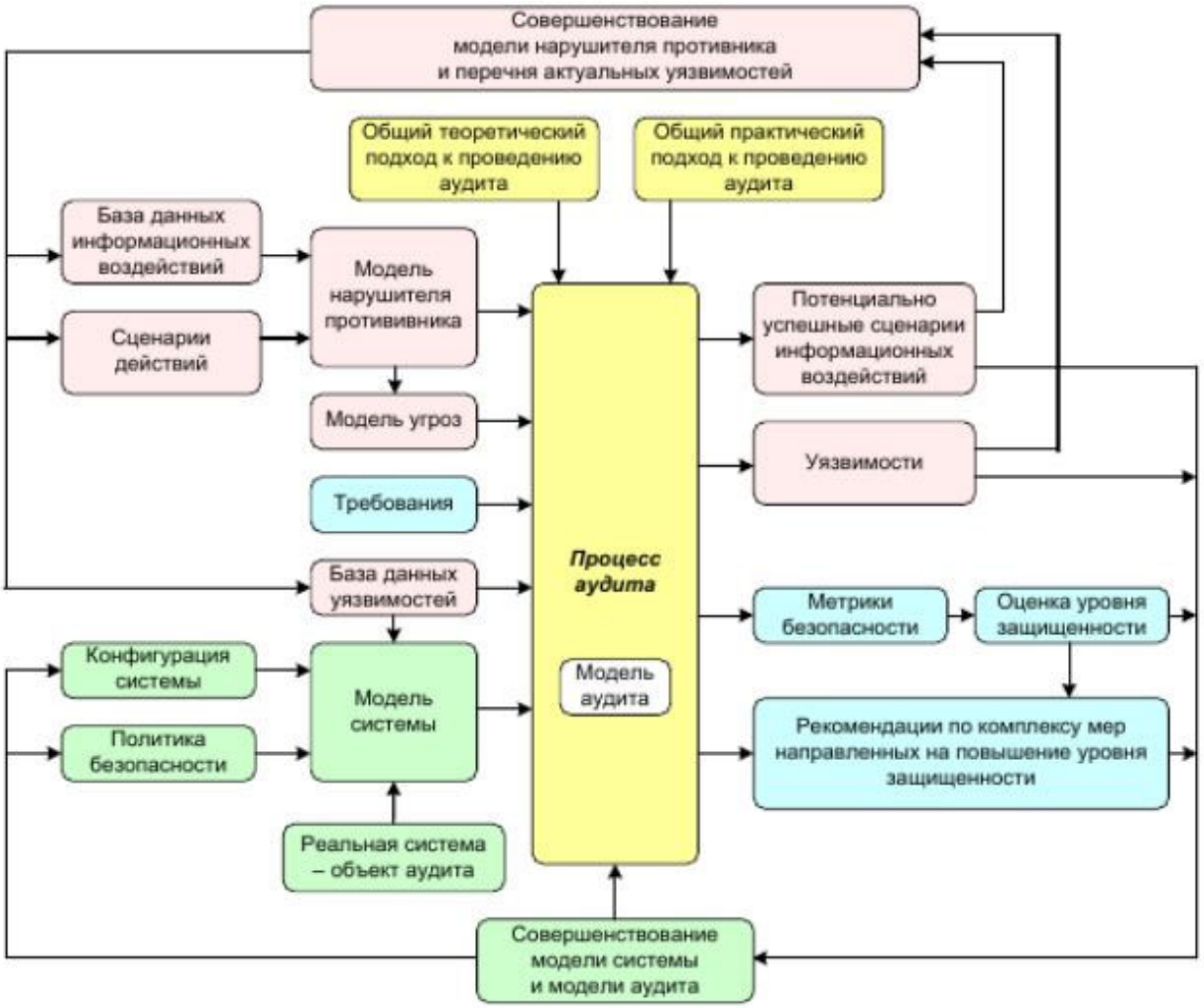

Рис. 1. Схема проведения аудита

Заключение

В данной работе рассмотрена проблема разработки методики аудита кибербезопасности ГИС, относящихся к ЗО КИИ, функционирующих на базе ЦОД.

Обозначена важность данной проблемы, описаны причины её возникновения, рассмотрены и обобщены существующие методики, а также сформулированы и поставлены цели и задачи для решения данной проблемы.

В дальнейшем будет разработана методика аудита кибербезопасности ГИС, относящихся к ЗО КИИ, функционирующих на базе ЦОД, и рекомендации по использованию этой методики.

Также будут разработаны критерии, используемые при проведении аудита кибербезопасности, на основе которых будет оцениваться защищенность свойств ИБ.

Значимость результатов обуславливается возможностью достаточно быстро, эффективно, с высокой точностью оценивать состояние защищенности ГИС систем в ходе государственного (межведомственного) контроля, учитывая разнообразие ИС и соблюдение соответствующих федеральных законов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Щелкин К.Е., Селифанов В.В., Звягинцева П.А. Возможные подходы к категорированию объектов критической информационной инфраструктуры. 2019. – С. 128-133. [Электронный ресурс] // Научная электронная библиотека «eLibrary». – Режим доступа: https://www.elibrary.ru/item.asp?id=41329277 (дата обращения: 05.03.2020).

2. Труфанов В.Н. Подход к созданию центров обработки персональных данных в организациях, обеспечивающих защиту государственных информационных ресурсов. 2018. – С. 56-62. [Электронный ресурс] // Научная электронная библиотека «eLibrary». – Режим доступа: https://www.elibrary.ru/item.asp?id=32651305 (дата обращения: 01.03.2020).

3. Козлов А.Г. О системе защиты информации. 2010. – С. 32-35. [Электронный ресурс] // Научная электронная библиотека «eLibrary». – Режим доступа: https://www.elibrary.ru/item.asp?id= 23143907 (дата обращения: 02.03.2020).

4. Будовских И.А. Оценка применимости для аудита безопасности государственных ИС методики определения угроз безопасности информации, разработанной ФСТЭК России 2016. – С. 240-243. [Электронный ресурс] // Научная электронная библиотека «eLibrary». – Режим доступа: https://www.elibrary.ru/item.asp?id= 26762949 (дата обращения: 02.03.2020).

5. Ермаков А.С. Методы аудита информационной безопасности государственного предприятия. 2017. – С. 10-14. [Электронный ресурс] // Научная электронная библиотека «eLibrary». – Режим доступа: https://www.elibrary.ru/item.asp?id= 25795345 (дата обращения: 02.03.2020).

6. Мальцев А.С Распространение методологии стандарта COBIT на проведение процедур по существу, выполняемых информационной системой аудита. 2015. – С. 57-59. [Электронный ресурс] // Научная электронная библиотека «eLibrary». – Режим доступа: https://www.elibrary.ru/item.asp?id= 24239204 (дата обращения: 02.03.2020).

7. Ромашова Л.В. Особенности государственного аудита информационной безопасности бизнес-систем. 2016. – С. 55-59. [Электронный ресурс] // Научная электронная библиотека «eLibrary». – Режим доступа: https://www.elibrary.ru/item.asp?id= 24984341 (дата обращения: 04.03.2020).

8. Каратунова Н.Г. Аудит комплексной и информационной безопасности объекта. 2017. – С. 63-65. [Электронный ресурс] // Научная электронная библиотека «eLibrary». – Режим доступа: https://www.elibrary.ru/item.asp?id= 29505431 (дата обращения: 04.03.2020).

9. Ситнов А.А. Организация аудита информационной безопасности. 2016. – С. 107- 110. [Электронный ресурс] // Научная электронная библиотека «eLibrary». – Режим доступа: https://www.elibrary.ru/item.asp?id= 28743214 (дата обращения: 04.03.2020).

10. Аверченков В.И. Аудит информационной безопасности, 3-е издание. 2016. – С.261-264. [Электронный ресурс] // Научная электронная библиотека «eLibrary». – Режим доступа: https://www.elibrary.ru/item.asp?id= 25083492 (дата обращения: 04.03.2020).

11. Порубель Т.В. Внутренний аудит и кибербезопасность. 2019. – С. 108-112. [Электронный ресурс] // Научная электронная библиотека «eLibrary». – Режим доступа: https://www.elibrary.ru/item.asp?id= 45398214 (дата обращения: 04.03.2020).

12. Сафонова М.Ф. Кибербезопасность: проблемы и решения. 2019. – С. 64- 68[Электронный ресурс] // Научная электронная библиотека «eLibrary». – Режим доступа: https://www.elibrary.ru/item.asp?id= 43024564 (дата обращения: 04.03.2020).

13. Хлестова Д.Р. Аудит информационной безопасности в организации. 2016. – С. 174-177. [Электронный ресурс] // Научная электронная библиотека «eLibrary». – Режим доступа: https://www.elibrary.ru/item.asp?id= 29233261 (дата обращения: 04.03.2020).

14. Исаев А.С. Границы применимости теории нечетких множеств при проведении аудита информационной безопасности. 2017. – С. 102-104. [Электронный ресурс] // Научная электронная библиотека «eLibrary». – Режим доступа: https://www.elibrary.ru/item.asp?id= 3001215 (дата обращения: 04.03.2020).

15. Федеральный закон №187 ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

16. Приказ ФСТЭК России от 21 декабря 2017 г. №235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

17. Приказ ФСТЭК России от 25 декабря 2017 г. №239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

18. Приказ ФСТЭК России от 11 февраля 2013 г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» с редакцией от 28 мая 2019 года.

19. Методический документ. Меры защиты в государственных информационных системах. Утвержден ФСТЭК России 11 февраля 2014 г.

20. Методический документ. Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении. Утвержден ФСТЭК России 11 февраля 2019 г.