УТВЕРЖДЕНЫ

руководством 8 Центра
ФСБ России

31 марта 2015 года

№ 149/7/2/6-432

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности

Введение

Настоящие методические рекомендации предназначены для федеральных органов исполнительной власти, осуществляющих функции по выработке государственной политики и нормативно-правовому регулированию в установленной сфере деятельности, органов государственной власти субъектов Российской Федерации, органов государственных внебюджетных фондов, иных государственных органов (далее – органы власти) которые, в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Закон), в пределах своих полномочий принимают нормативные правовые акты, в которых определяют угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных (далее – ИСПДн), эксплуатируемых при осуществлении соответствующих видов деятельности, с учетом содержания персональных данных, характера и способов их обработки (далее – НПА).

В методических рекомендациях отражены только необходимые для включения в проекты НПА положения, находящиеся в компетенции ФСБ России.

Настоящими методическими рекомендациями целесообразно также руководствоваться при разработке частных моделей угроз операторам информационных систем персональных данных, принявшим решение об использовании средств криптографической защиты информации (далее – СКЗИ) для обеспечения безопасности персональных данных.

1. Общее описание информационных систем персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности

В проекте НПА целесообразно, в первую очередь, привести перечень и общее описание информационных систем персональных данных, которые могут эксплуатироваться операторами при осуществлении соответствующих видов деятельности и (по возможности) определить уровни защищенности для таких информационных систем в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

Возможны три случая:

1. ИСПДн имеют сходную структуру, однотипны. В дальнейшем такие системы будут именоваться «однотипными системами». Примером может служить описание федеральным органом исполнительной власти угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах территориальных подразделений этого органа.

В указанном случае целесообразно в проекте НПА указывать наиболее полную информацию об ИСПДн и среде их функционирования.

Следует отметить, что в зависимости от вида деятельности, для которого разрабатывается НПА, в проекте НПА может выделяться несколько категорий однотипных систем.

2. ИСПДн разноплановы, имеют различную структуру и могут содержать различные категории персональных данных. В дальнейшем такие системы будут именоваться «разноплановыми системами».

В этом случае целесообразно перечислить имеющиеся системы и указать общую информацию о возможной среде их функционирования, если такая информация имеется.

3. Эксплуатируются как одна или несколько однотипных, так и разноплановые системы.

В этом случае целесообразно указывать наиболее полную информацию о категориях однотипных систем и среде их функционирования, а также общую информацию о разноплановых системах и среде их функционирования.

При описании информационных систем следует, в частности, указывать:

– общие сведения об информационных системах (назначение, оператор (уполномоченное лицо);

– объем и содержание персональных данных, обрабатываемых в информационных системах;

– характеристики безопасности (конфиденциальность, целостность, доступность, подлинность), которые необходимо обеспечивать для обрабатываемых персональных данных.

При описании однотипных систем следует также указывать:

– объекты, в которых размещены ресурсы информационных систем;

– физические меры защиты объектов, в которых размещены ресурсы информационных систем;

– меры по обеспечению контролируемой зоны;

– типы информационных систем (например, единая информационная система для всех обрабатываемых персональных данных или совокупность изолированных и (или) взаимосвязанных информационных подсистем. В последнем случае необходимо приводить описание взаимосвязей между подсистемами и указывать объем и содержание персональных данных, обрабатываемых в каждой подсистеме);

– наличие или отсутствие информационного взаимодействия каждой подсистемы информационной системы или информационной системы в целом с другими информационными системами, а также наличие факта передачи персональных данных между ними;

– используемые в каждой подсистеме или в информационной системе в целом каналы (линии) связи, включая кабельные системы, и меры по ограничению несанкционированного доступа к защищаемой информации, передаваемой по этим каналам (линиям) связи, с указанием каналов (линий) связи, в которых невозможен несанкционированный доступ к передаваемой по ним защищаемой информации, и реализуемые для обеспечения этого качества меры;

– носители защищаемой информации, используемые в каждой подсистеме информационной системы или в информационной системе в целом (за исключением каналов (линий) связи).

2. Определение актуальности использования СКЗИ для обеспечения безопасности персональных данных

Использование СКЗИ для обеспечения безопасности персональных данных необходимо в следующих случаях:

- если персональные данные подлежат криптографической защите в соответствии с законодательством Российской Федерации;

- если в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ.

Кроме того, решение о необходимости криптографической защиты персональных данных может быть принято конкретным оператором на основании технико-экономического сравнения альтернативных вариантов обеспечения требуемых характеристик безопасности информации, содержащей, в том числе, персональные данные.

К случаям, когда угрозы могут быть нейтрализованы только с помощью СКЗИ, относятся:

- передача персональных данных по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при

передаче персональных данных по информационно-телекоммуникационным сетям общего пользования);

- хранение персональных данных на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов.

При этом необходимо учитывать следующее:

– криптографическая защита персональных данных может быть обеспечена при условии отсутствия возможности несанкционированного доступа нарушителя к ключевой информации СКЗИ;

– СКЗИ штатно функционируют совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к СКЗИ требований и которые образуют среду функционирования СКЗИ;

– СКЗИ не предназначены для защиты информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СКЗИ не предназначены для защиты персональных данных от раскрытия лицами, которым предоставлено право на доступ к этой информации);

– СКЗИ обеспечивают защиту информации при условии соблюдения требований эксплуатационно-технической документации на СКЗИ и требований действующих нормативных правовых документов в области реализации и эксплуатации СКЗИ;

– для обеспечения безопасности персональных данных при их обработке в ИСПДн должны использоваться СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия. Перечень СКЗИ, сертифицированных ФСБ России, опубликован на официальном сайте Центра по лицензированию, сертификации и защите государственной тайны ФСБ России (www.clsz.fsb.ru). Дополнительную информацию о конкретных средствах защиты информации рекомендуется получать непосредственно у

разработчиков или производителей этих средств и, при необходимости, у специализированных организаций, проводивших тематические исследования этих средств;

– в случае отсутствия прошедших в установленном порядке процедуру оценки соответствия СКЗИ, функционально пригодных для обеспечения безопасности персональных данных при их обработке в конкретной информационной системе, на этапе аванпроекта или эскизного (эскизно-технического) проекта разработчиком информационной системы с участием оператора (уполномоченного лица) и предполагаемого разработчика СКЗИ готовится обоснование целесообразности разработки нового типа СКЗИ и определяются требования к его функциональным свойствам. Решение о разработке нового типа СКЗИ может быть принято оператором в инициативном порядке в независимости от наличия СКЗИ, функционально пригодных для обеспечения безопасности персональных данных при их обработке в конкретной ИСПДн. Разработка нового типа СКЗИ осуществляется в соответствии с Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации, утвержденным приказом ФСБ России от 9 февраля 2005 г. № 66 (далее – Положение ПКЗ-2005);

– СКЗИ являются как средством защиты персональных данных, так и объектом защиты.

3. Определение актуальных угроз

В случае, если для информационных систем персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, угрозы, которые могут быть нейтрализованы только с помощью СКЗИ, неактуальны, изложенные в настоящем разделе угрозы могут не учитываться при разработке НПА.

При использовании каналов (линий) связи, с которых невозможен перехват передаваемой по ним защищаемой информации и (или) в которых невозможно осуществление несанкционированных воздействий на эту информацию, при общем описании информационных систем необходимо указывать:

– описание методов и способов защиты этих каналов от несанкционированного доступа к ним;

– выводы по результатам исследований защищенности этих каналов (линий) связи от несанкционированного доступа к передаваемой по ним защищенной информации организацией, имеющей право проводить такие исследования, со ссылкой на документ, в котором содержатся эти выводы.

В случае, если НПА разрабатывается только для разноплановых систем, и при этом угрозы, которые могут быть нейтрализованы только с помощью СКЗИ, являются актуальными, изложенные ниже угрозы могут не учитываться при разработке НПА. При этом необходимо указать операторам о необходимости разработки для имеющихся ИСПДн частных моделей угроз с учетом настоящего раздела.

В случае, если НПА разрабатывается только для однотипных систем, и при этом угрозы, которые могут быть нейтрализованы только с помощью СКЗИ актуальны, изложенные в настоящем разделе угрозы в обязательном порядке должны быть учтены при разработке НПА.

При этом, в описании информационных систем необходимо указывать:

– меры по разграничению доступа в помещения, в которых размещены ресурсы информационной системы, имеющие отношение к криптографической защите персональных данных;

– информационные технологии, базы данных, технические средства, программное обеспечение, используемые в каждой подсистеме информационной системы или в информационной системе в целом для

обработки персональных данных и имеющие отношение к криптографической защите персональных данных;

– отчуждаемые носители защищаемой информации, используемые в каждой подсистеме информационной системы или в информационной системе в целом, для которых несанкционированный доступ к хранимой на них информации не может быть исключен без использования криптографических методов и способов;

– область применения СКЗИ в информационной системе и цели применения СКЗИ в информационной системе.

В случае, если с учетом соответствующего вида деятельности в НПА необходимо отразить актуальные угрозы как для одной или нескольких категорий однотипных, так и для разноплановых систем, и при этом угрозы, которые могут быть нейтрализованы только с помощью СКЗИ актуальны, проект НПА должен содержать раздел о рассмотрении изложенных ниже угроз для категорий однотипных систем и указание операторам о необходимости разработки с учетом настоящего раздела частных моделей для разноплановых систем. В случае если оператор определил, что применение СКЗИ необходимо для обеспечения безопасности персональных данных в различных сегментах информационной системы персональных данных, то класс СКЗИ определяется для каждого объекта защиты в рамках одной информационной системы персональных данных. В случае применения СКЗИ для обеспечения безопасности различных объектов защиты, возможно в рамках одной информационной системы персональных данных использовать СКЗИ разных классов.

В случае, если угрозы, которые могут быть нейтрализованы только с помощью СКЗИ, актуальны или принято решение об использовании СКЗИ для обеспечения безопасности персональных данных вне зависимости от актуальности таких угроз, помимо исходных данных об информационных системах необходимо описать:

- объекты защиты и актуальные характеристики безопасности объектов защиты угрозы;

- классификация и характеристики нарушителей, а также их возможностей по реализации атак;

- источники атак.

3.1 К объектам защиты, кроме персональных данных, относятся:

– СКЗИ;

– среда функционирования СКЗИ (далее - СФ);

– информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;

– документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация, относящаяся к информационным системам персональных данных и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты СФ;

– носители защищаемой информации, используемые в информационной системе в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;

– используемые информационной системой каналы (линии) связи, включая кабельные системы;

– помещения, в которых находятся ресурсы информационной системы, имеющие отношение к криптографической защите персональных данных.

Описание объектов защиты должно отражать специфику информационной системы.

3.2 При описании источников атак определяются категории физических лиц, имеющих право постоянного или разового доступа в контролируемую зону информационной системы.

К отдельной категории относятся привилегированные пользователи информационной системы (члены группы администраторов), которые назначаются из числа доверенных лиц и осуществляют техническое обслуживание технических и программных средств СКЗИ и СФ, включая их настройку, конфигурирование и распределение ключевой документации между непривилегированными пользователями.

Определяется возможность или невозможность доступа лиц каждой категории к объектам защиты.

Кроме того, определяется и обосновывается перечень категорий лиц, которые не рассматриваются в качестве потенциальных источников атак, перечень категорий лиц, которые рассматриваются в качестве потенциальных источников атак, а также констатируется наличие внешних источников атак (без их характеристики) и возможность или невозможность доступа внешних источников атак к объектам защиты.

На основании исходных данных об информационных системах, объектах защиты и источниках атак заполняется Таблица № 1 об обобщенных возможностях источников атак.

Таблица № 1

№	Обобщенные возможности источников атак	Да/нет
1	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	
2	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее – АС), на которых реализованы СКЗИ и среда их функционирования	

3	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования	
4	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	
5	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения);	
6	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ).	

При этом заполнение пунктов 4, 5 и 6 Таблицы № 1 должно осуществляться с учетом объема и содержания обрабатываемых в информационных системах персональных данных, и результатов произведенной во исполнение пункта 5 части 1 статьи 18 [1] Закона оценке возможного вреда субъекту персональных данных.

3.3 Реализация угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных, определяется возможностями источников атак. Таким образом, актуальность использования возможностей источников атак определяет наличие соответствующих актуальных угроз.

В зависимости от положительных ответов в Таблице № 1 следует заполнить Таблицу № 2 по следующим правилам:

В случае, если выбрана только обобщенная возможность № 1, то в Таблице № 2 необходимо привести обоснование признания угроз 1.1-4.3 неактуальными.

При обосновании неактуальности угроз следует приводить перечень организационно-технических мер, реализация которых позволяет нейтрализовать такие угрозы, или особенности функционирования и организации эксплуатации информационной системы, делающие такие угрозы неактуальными.

Пример заполнения Таблицы № 2 в случае выбора обобщенной возможности № 1 приведен в Приложении № 1.

В случае, если в Таблице № 1 максимально выбранная обобщенная возможность не выше № 2, то в Таблице № 2 обязательно актуальна хотя бы одна из угроз 1.1-1.4, а также необходимо привести обоснование признания угроз 2.1-4.3 неактуальными.

В случае, если в Таблице № 1 максимально выбранная обобщенная возможность не выше № 3, то в Таблице № 2 обязательно актуальна хотя бы одна из угроз 1.1-2.2, а также необходимо привести обоснование признания угроз 3.1-4.3 неактуальными.

В случае, если в Таблице № 1 максимально выбранная обобщенная возможность не выше № 5, то в Таблице № 2 обязательно актуальна хотя бы одна из угроз 1.1-3.3, а также необходимо привести обоснование признания угроз 4.1-4.3 неактуальными.

Пример заполнения Таблицы № 2 в случае выбора обобщенной возможности № 5 приведен в Приложении № 2.

В случае, если в Таблице № 1 выбрана обобщенная возможность № 6, то заполнять Таблицу № 2 нет необходимости.

Таблица № 2

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и	Обоснование отсутствия

		реализации атак	
1.1	проведение атаки при нахождении в пределах контролируемой зоны		
1.2	проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ;		
1.3	получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: - сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ;		
1.4	использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.		
2.1	физический доступ к СВТ, на которых реализованы СКЗИ и СФ;		

2.2	возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.		
3.1	создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО;		
3.2	проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий;		
3.3	проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ.		
4.1	создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей		

	системного ПО;		
4.2	возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ;		
4.3	возможность воздействовать на любые компоненты СКЗИ и СФ.		

В случае, если по результатам заполнения Таблицы № 2 выявляется отсутствие организационно-технических мер в рассматриваемой информационной системе, реализация которых позволяет нейтрализовать рассматриваемую угрозу, или отсутствует обоснование отсутствия такой угрозы в связи с особенностями функционирования информационной системы, то такая угроза признается актуальной. В таком случае следует пересмотреть выбор обобщенных возможностей в Таблице № 1 и повторить заполнение Таблицы № 2 с учетом выбора новых обобщенных возможностей.

Заключение

В соответствии с частью 7 статьи 19 Закона проекты НПА подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации.

Согласование с ФСБ России частных моделей угроз операторов, подготовленных в соответствии с настоящими методическими рекомендациями, не требуется.

Приложение № 1

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1.1	проведение атаки при нахождении в пределах контролируемой зоны.	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены СКЗИ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; сотрудники, являющиеся пользователями ИСПДн, но не являющиеся пользователями СКЗИ, проинформированы о правилах работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации; пользователи СКЗИ проинформированы о правилах работы в ИСПДн, правилах работы с СКЗИ и ответственности за несоблюдение правил обеспечения безопасности информации; помещения, в которых располагаются СКЗИ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода; утверждены правила доступа в помещения, где располагаются СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях; утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей с ПДн; осуществляется контроль целостности средств защиты; на АРМ и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты.
1.2	проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе; помещение, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода; утвержден перечень лиц, имеющих право доступа в

	СКЗИ и СФ.		помещения.
1.3	получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: - сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по разграничению доступа в Помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ.	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается ресурсы ИСПДн, обеспечивается в соответствии с контрольно-пропускным режимом; сведения о физических мерах защиты объектов, в которых размещены ИСПДн, доступны ограниченному кругу сотрудников; сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации.
1.4	использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	не актуально	проводятся работы по подбору персоналов; помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода; сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; в ИСПДн используются: сертифицированные средства защиты информации от несанкционированного доступа; сертифицированные средства антивирусной защиты.
2.1	физический доступ к СВТ, на которых реализованы СКЗИ и СФ.	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода.
2.2	возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компонентыСКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии

			сотрудников по эксплуатации.
3.1	создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО.	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности; проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компонентыСКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; на АРМ и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты.
3.2	проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности.
3.3	проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ.	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности.
4.1	создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО.	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности; проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и

			СФ, обеспечивается в соответствии с контрольно-пропускным режимом; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытия дверей помещений на замок и их открытия только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; на АРМ и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты.
4.2	возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ.	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.
4.3	возможность воздействовать на любые компоненты СКЗИ и СФ.	не актуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.

Приложение № 2

№	Уточнённые возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1.1	проведение атаки при нахождении в пределах контролируемой зоны.	не актуально	
1.2	проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ.	не актуально	
1.3	получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации: - сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по разграничению доступа в Помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ.	не актуально	
1.4	использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	не актуально	
2.1	физический доступ к СВТ, на которых реализованы СКЗИ и СФ.	не актуально	
2.2	возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	актуально	
3.1	создание способов, подготовка и проведение атак с привлечением	актуально	

	специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО.		
3.2	проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	не актуально	
3.3	проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ.	не актуально	
4.1	создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО.	не актуально	наличие заключения об отсутствии недекларированных возможностей системного ПО.
4.2	возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ.	не актуально	высокая стоимость и сложность подготовки реализации возможности.
4.3	возможность воздействовать на любые компоненты СКЗИ и СФ.	не актуально	высокая стоимость и сложность подготовки реализации возможности; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам.