Вопрос 2. Порядок оценки угроз безопасности информации

2.1. 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.

2.2. Основными задачами, решаемыми в ходе оценки угроз безопасности информации, являются:

а) определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;

б) инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;

в) определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;

г) оценка способов реализации (возникновения) угроз безопасности информации;

д) оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;

е) оценка сценариев реализации угроз безопасности информации в системах и сетях.

2.3. Исходными данными для оценки угроз безопасности информации являются:

а) общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

б) описания векторов (шаблоны) компьютерных атак, содержащиеся в базах данных и иных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.);

в) документация на системы и сети (а именно: техническое задание на создание систем и сетей, частное техническое задание на создание системы защиты, программная (конструкторская) и эксплуатационная (руководства, инструкции) документация, содержащая сведения о назначении и функциях, составе и архитектуре систем и сетей, о группах пользователей и уровне их полномочий и типах доступа, о внешних и внутренних интерфейсах, а также иные документы на системы и сети, разработка которых предусмотрена требованиями по защите информации (обеспечению безопасности) или национальными стандартами);

г) договоры, соглашения или иные документы, содержащие условия использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (в случае функционирования систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры);

д) нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и функционируют системы и сети, содержащие в том числе описание назначения, задач (функций) систем и сетей, состав обрабатываемой информации и ее правовой режим;

е) технологические, производственные карты или иные документы, содержащие описание управленческих, организационных, производственных и иных основных процессов (бизнес-процессов) в рамках выполнения функций (полномочий) или осуществления видов деятельности обладателя информации, оператора (далее - основные (критические) процессы);

ж) результаты оценки рисков (ущерба), проведенной обладателем информации и (или) оператором.

Указанные исходные данные могут уточняться или дополняться с учетом особенностей области деятельности, в которой функционируют системы и сети.

2.4. Оценка угроз безопасности информации должна носить систематический характер и осуществляться как на этапе создания систем и сетей, так и в ходе их эксплуатации, в том числе при развитии (модернизации) систем и сетей. Систематический подход к оценке угроз безопасности информации позволит поддерживать адекватную и эффективную систему защиты в условиях изменения угроз безопасности информации и информационных ресурсов и компонентов систем и сетей. Учет изменений угроз безопасности информации обеспечит своевременную выработку адекватных и эффективных мер по защите информации (обеспечению безопасности) в системах и сетях.

2.5. На этапе создания систем и сетей оценка угроз безопасности информации проводится на основе их предполагаемых архитектуры и условий функционирования, определенных по результатам изучения и анализа исходных данных на них. В ходе эксплуатации систем и сетей, в том числе при развитии (модернизации) систем и сетей, оценка угроз безопасности информации проводится для реальной архитектуры систем и сетей и условий их функционирования, полученных по результатам анализа исходных данных, инвентаризации информационных ресурсов, анализа уязвимостей и (или) тестирования на проникновение систем и сетей, а также иных методов исследований уровня защищенности систем и сетей и содержащейся в них информации.

2.6. По результатам оценки, проведенной в соответствии с Методикой оценки угроз безопасности информации, должны быть выявлены актуальные угрозы безопасности информации, реализация (возникновение) которых может привести к нарушению безопасности обрабатываемой в системах и сетях информации (нарушению конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации и (или) средств ее обработки) и (или) к нарушению, прекращению функционирования систем и сетей.

На этапе создания систем и сетей результаты оценки угроз безопасности информации должны быть направлены на обоснование выбора организационных и технических мер по защите информации (обеспечению безопасности), а также на выбор средств защиты информации и их функциональных возможностей.

На этапе эксплуатации систем и сетей результаты оценки угроз безопасности информации должны быть направлены на оценку эффективности принятых технических мер, в том числе используемых средств защиты информации.

2.7. Оценка угроз безопасности информации проводится подразделением по защите информации (отдельными специалистами, назначенными ответственными за обеспечение защиты информации (обеспечение безопасности)) обладателя информации или оператора с участием подразделений или специалистов, ответственных за эксплуатацию систем и сетей (ИТ-специалистов, специалистов автоматизированных систем управления, специалистов связи и др.), основных (профильных) подразделений обладателя информации или оператора. Для оценки угроз безопасности информации по решению обладателя информации или оператора в соответствии с законодательством Российской Федерации могут привлекаться специалисты сторонних организаций.

Для оценки угроз безопасности информации рекомендуется привлекать специалистов, обладающих следующими знаниями и умениями:

а) основ оценки рисков, а также основных рисков от нарушения функционирования систем и сетей и нарушения безопасности обрабатываемой информации (далее - информационные риски);

б) угроз безопасности информации и способов их реализации (возникновения);

в) тактик и техник проведения компьютерных атак (реализации угроз безопасности информации);

г) основных типов компьютерных инцидентов и причин их возникновения;

д) основных уязвимостей систем и сетей;

е) нормативных правовых актов по созданию и функционированию систем и сетей, защите информации (обеспечению безопасности) в них, основных (критических) процессов (бизнес-процессов) обладателя информации и (или) оператора;

ж) оценивать информационные риски;

з) классифицировать и оценивать угрозы безопасности информации;

и) определять сценарии (тактики, техники) реализации угроз безопасности информации;

к) определять источники и причины возникновения компьютерных инцидентов;

л) проводить инвентаризацию систем и сетей, анализ уязвимостей, тестирование на проникновение систем и сетей с использованием соответствующих автоматизированных средств;

м) оценку уровня защищенности (аудит) систем и сетей и содержащейся в них информации.

2.8. Оценка угроз безопасности информации проводится с использованием экспертного метода. В интересах снижения субъективных факторов при оценке угроз безопасности информации рекомендуется создавать экспертную группу. Рекомендации по формированию экспертной группы и проведению экспертной оценки угроз безопасности информации приведены в приложении 2 к Методике оценки угроз безопасности информации.

2.9. При оценке угроз безопасности информации могут использоваться программные средства, позволяющие автоматизировать данную деятельность.

Для получения (уточнения) отдельных исходных данных (например, объектов воздействия и их интерфейсов, уязвимостей) в интересах оценки угроз безопасности информации на этапе эксплуатации систем и сетей применяются автоматизированные средства инвентаризации систем и сетей, анализа уязвимостей, тестирования на проникновение систем и сетей, а также иные средства, используемые для исследований уровня защищенности систем и сетей и содержащейся в них информации.

2.10. В случае оценки угроз безопасности информации для систем и сетей, функционирующих на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, угрозы безопасности информации определяются как для самих систем и сетей, так и для информационно-телекоммуникационной инфраструктуры, на которой они функционируют (рисунок 1).

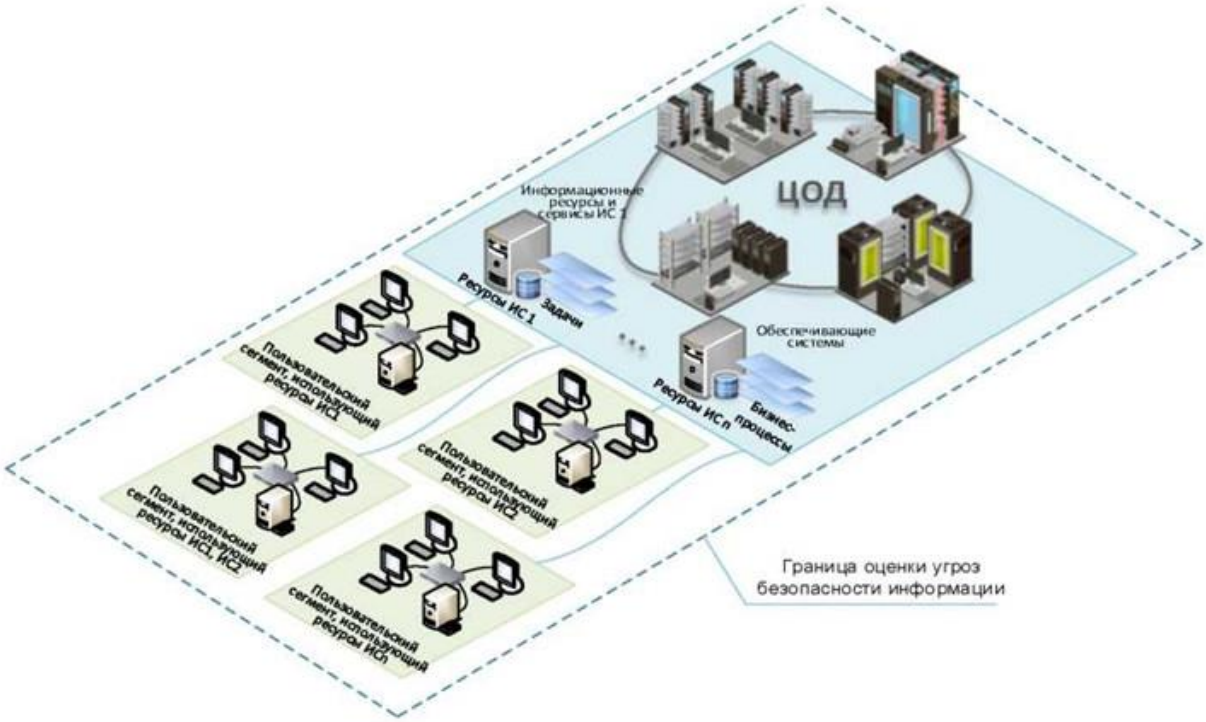

Рисунок 1. Оценка угроз безопасности информации в информационной инфраструктуре на базе центра обработки данных

2.11. При размещении систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, принадлежащей поставщику услуг, оценка угроз безопасности информации проводится оператором во взаимодействии с поставщиком услуг.

В случае размещения систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, для которой поставщик услуг не оценил угрозы безопасности информации или не представил результаты такой оценки, оператор при оценке угроз безопасности информации исходит из предположения, что информационно-телекоммуникационная инфраструктура центра обработки данных или облачная инфраструктура, являющаяся средой функционирования для его систем и сетей, подвержена угрозам безопасности информации (скомпрометирована нарушителем с максимальным уровнем возможностей).

2.12. Результаты оценки угроз безопасности информации отражаются в модели угроз, которая представляет собой описание систем и сетей и актуальных угроз безопасности информации. Рекомендуемая структура модели угроз безопасности информации приведена в приложении 3 к Методике оценки угроз безопасности информации.

2.13. По решению обладателя информации или оператора модель угроз безопасности информации разрабатывается как для отдельной системы или сети, так и для совокупности взаимодействующих систем и сетей оператора. При разработке модели угроз безопасности информации для отдельной системы и сети, она должна содержать описание угроз безопасности информации, актуальных для информационно-телекоммуникационной инфраструктуры, на базе которой эта система или сеть функционирует, а также угроз безопасности информации, связанных с интерфейсами взаимодействия со смежными (взаимодействующими) системами и сетями.

Допускается разработка одной модели угроз безопасности информации для нескольких однотипных создаваемых систем и сетей обладателя информации или оператора.

2.14. Модель угроз безопасности информации должна поддерживаться в актуальном состоянии в процессе функционирования систем и сетей.

Ведение модели угроз безопасности информации и поддержание ее в актуальном состоянии может осуществляться в электронном виде с учетом приложения 3 к Методике оценки угроз безопасности информации.

Изменение модели угроз безопасности информации осуществляется в случаях:

а) изменения требований нормативных правовых актов Российской Федерации, методических документов ФСТЭК России, регламентирующих вопросы оценки угроз безопасности информации;

б) изменений архитектуры и условий функционирования систем и сетей, режима обработки информации, правового режима информации, влияющих на угрозы безопасности информации;

в) выявления, в том числе по результатам контроля уровня защищенности систем и сетей и содержащейся в них информации (анализа уязвимостей, тестирований на проникновение, аудита), новых угроз безопасности информации или новых сценариев реализации существующих угроз;

г) включения в банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru) сведений о новых угрозах безопасности информации, сценариях (тактиках, техниках) их реализации.

2.15. Оценка угроз безопасности информации включает следующие этапы:

1) определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;

2) определение возможных объектов воздействия угроз безопасности информации;

3) оценку возможности реализации (возникновения) угроз безопасности информации и определение их актуальности.

Общая схема проведения оценки угроз безопасности информации приведена на рисунке 2.

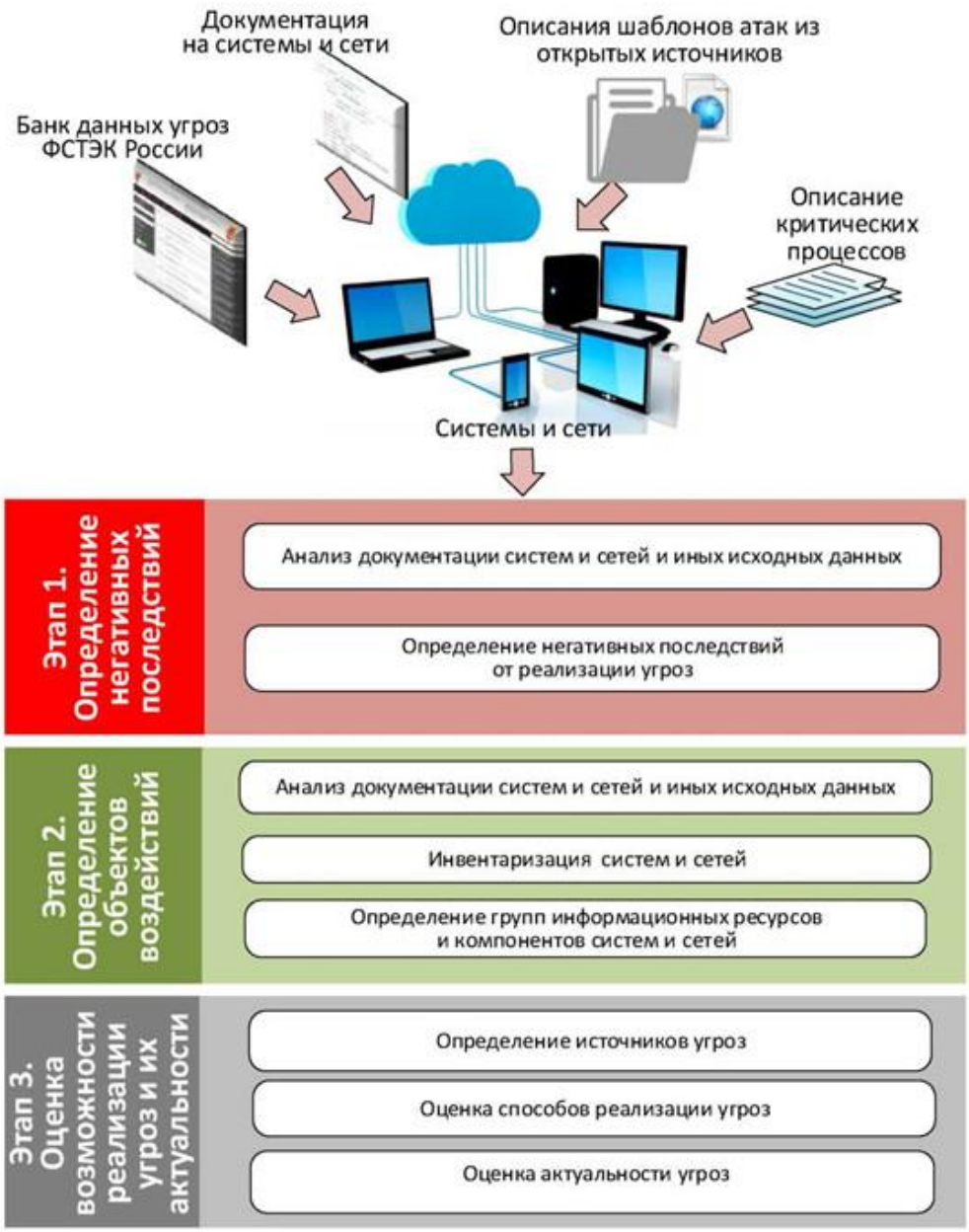

Рисунок 2. Общая схема проведения оценки угроз безопасности информации

РЕКОМЕНДАЦИИ ПО ФОРМИРОВАНИЮ ЭКСПЕРТНОЙ ГРУППЫ И ПРОВЕДЕНИЮ ЭКСПЕРТНОЙ ОЦЕНКИ ПРИ ОЦЕНКЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ (Приложение 2 к Методике оценки угроз безопасности информации).

Качественное формирование экспертной группы способствует снижению субъективных факторов при оценке угроз безопасности информации. Занижение (ослабление) экспертами прогнозов и предположений при оценке угроз может повлечь наступление непрогнозируемого (неожиданного) ущерба в результате их реализации. Завышение экспертами прогнозов и предположений при моделировании угроз безопасности информации может повлечь за собой неоправданные расходы на нейтрализацию (блокирование) угроз, являющихся неактуальными.

Независимо от результата формирования экспертной группы при оценке угроз безопасности информации существуют субъективные факторы, связанные с психологией принятия решений. Это также может приводить как к занижению (ослаблению), так и к

завышению (усилению) экспертами прогнозов и предположений при оценке угроз безопасности информации, что в свою очередь может привести к пропуску отдельных угроз безопасности информации или к неоправданным затратам на нейтрализацию неактуальных угроз.

Любое решение, принимаемое экспертами при оценке угроз безопасности информации, должно исходить из правил, при которых нарушитель находится в наилучших условиях для реализации угрозы безопасности (принципа «гарантированности»).

а) формирование экспертной группы

В состав экспертной группы для оценки угроз безопасности информации рекомендуется включать экспертов (независимо от того, реализуются ли функции обладателя информации, заказчика и оператора в рамках одной или нескольких организаций) от:

подразделения по защите информации (обеспечения информационной безопасности);

подразделения, ответственного за цифровую трансформацию (ИТ-специалистов);

подразделения, ответственного за эксплуатацию сетей связи;

подразделения, ответственного за эксплуатацию автоматизированных систем управления;

подразделений обладателя информации или оператора, ответственного за выполнение основных (критических) процессов (бизнес-процессов).

Состав экспертов по решению обладателя информации или оператора может быть дополнен или уточнен с учетом особенностей области деятельности, в которой функционируют системы и сети. В частности, для оценки угроз безопасности информации, реализация которых может привести к финансовым рискам, рекомендуется привлекать дополнительно специалистов экономических (финансовых) подразделений обладателя информации или оператора.

Для организации работы экспертной группы рекомендуется определять специалиста по защите информации (обеспечению информационной безопасности), имеющего стаж работ не менее трех лет и практический опыт оценки информационных рисков. В экспертную группу для оценки угроз безопасности информации рекомендуется включать специалистов, имеющих опыт работы не менее одного года по соответствующему направлению деятельности, в котором проводится оценка угроз безопасности информации.

Эксперты должны обладать независимостью, основанной на отсутствии коммерческого и финансового интереса или другого давления, которое может оказать влияние на принимаемые решения. Не рекомендуется формировать экспертную группу из участников, находящихся в прямом подчинении, так как это может негативным образом повлиять на результат определения угроз безопасности информации.

В состав экспертной группы должны входить не менее трех экспертов.

б) проведение экспертной оценки

При проведении экспертной оценки принимаются меры, направленные на снижение уровня субъективности и неопределенности при определении каждой из угроз безопасности информации.

Экспертную оценку рекомендуется проводить в отношении следующих параметров:

а) негативного последствия от реализации угроз безопасности информации;

б) целей нарушителей по реализации угроз безопасности информации;

в) сценария действий нарушителей при реализации угроз безопасности информации.

Оценку параметров рекомендуется проводить опросным методом с составлением анкеты, в которой указываются вопросы и возможные варианты ответа в единой принятой шкале измерений («низкий», «средний», «высокий» или «да», «нет» или иные шкалы). При этом вопросы должны быть четкими и однозначно трактуемыми, предполагать однозначные ответы.

Опрос экспертов включает следующие этапы:

каждый эксперт проводит оценку оцениваемого параметра (рекомендуется не менее двух раундов оценки), результаты которой заносятся в таблицу;

после оценки каждым из экспертов отбрасываются минимальные и максимальные значения;

определяется среднее значение оцениваемого параметра в каждом раунде;

определяется итоговое среднее значение оцениваемого параметра.

Пример таблицы результатов оценки параметров

Эксперты	Значение оцениваемого параметра (раунд 1)	Значение оцениваемого параметра (раунд 2)
Эксперт 1		
Эксперт 2		
Эксперт n		
Итоговое значение		

РЕКОМЕНДУЕМАЯ СТРУКТУРА МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ (Приложение 3 к Методике оценки угроз безопасности информации).

УТВЕРЖДАЮ

Руководитель органа государственной власти
(организации) или иное
уполномоченное лицо
_____
«__» _____ 20__ г.

Модель угроз безопасности информации
«_____»
наименование системы и (или) сети

1. Общие положения

Раздел «Общие положения» содержит:

назначение и область действия документа;

нормативные правовые акты, методические документы, национальные стандарты, используемые для оценки угроз безопасности информации и разработки модели угроз;

наименование обладателя информации, заказчика, оператора систем и сетей;

подразделения, должностные лица, ответственные за обеспечение защиты информации (безопасности) систем и сетей;

наименование организации, привлекаемой для разработки модели угроз безопасности информации (при наличии).

2. Описание систем и сетей и их характеристика как объектов защиты

Раздел «Описание систем и сетей и их характеристика как объектов защиты» содержит:

наименование систем и сетей, для которых разработана модель угроз безопасности информации;

класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных;

нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети;

назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим;

основные процессы (бизнес-процессы) обладателя информации, оператора, для обеспечения которых создаются (функционируют) системы и сети;

состав и архитектуру систем и сетей, в том числе интерфейсы и взаимосвязи компонентов систем и сетей;

описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа (в состав групп пользователей включаются все пользователи, для которых требуется авторизация при доступе к информационным ресурсам, и пользователи, для которых не требуется авторизация (например, предоставлен доступ к сайту без прохождения авторизации);

описание внешних интерфейсов и взаимодействий систем и сетей с пользователями (в том числе посредством машинных носителей информации, средств ввода-вывода, веб-приложений), иными системами и сетями, обеспечивающими системами, в том числе с сетью «Интернет»;

информацию о функционировании систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, о модели предоставления вычислительных услуг, о распределении ответственности за защиту информации между обладателем информации, оператором и поставщиком вычислительных услуг, об условиях использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (при наличии).

К модели угроз безопасности информации могут прилагаться схемы и рисунки, иллюстрирующие состав и архитектуру систем и сетей, интерфейсы взаимодействия компонентов системы и сети, группы пользователей, а также другие поясняющие материалы.

3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации

Раздел «Возможные негативные последствия от реализации (возникновения) угроз безопасности информации» содержит:

описание видов рисков (ущербов), актуальных для обладателя информации, оператора, которые могут наступить от нарушения или прекращения основных процессов;

описание негативных последствий, наступление которых в результате реализации (возникновения) угроз безопасности информации может привести к возникновению рисков (ущерба).

4. Возможные объекты воздействия угроз безопасности информации

Раздел «Возможные объекты воздействия угроз безопасности информации» содержит:

наименования и назначение компонентов систем и сетей, которые непосредственно участвуют в обработке и хранении защищаемой информации, или обеспечивают реализацию основных процессов обладателя информации, оператора;

описание видов воздействия на компоненты систем и сетей, реализация которых нарушителем может привести к негативным последствиям.

К модели угроз безопасности информации может прилагаться схема с отображением объектов воздействия и их назначения в составе архитектуры систем и сетей.

5. Источники угроз безопасности информации

Раздел «Источники угроз безопасности информации» содержит:

характеристику нарушителей, которые могут являться источниками угроз безопасности информации, и возможные цели реализации ими угроз безопасности информации;

категории актуальных нарушителей, которые могут являться источниками угроз безопасности информации;

описание возможностей нарушителей по реализации ими угроз безопасности применительно к назначению, составу и архитектуре систем и сетей.

К модели угроз безопасности информации могут прилагаться рисунки, иллюстрирующие возможности нарушителей, и другие поясняющие материалы.

6. Способы реализации (возникновения) угроз безопасности информации

Раздел «Способы реализации (возникновения) угроз безопасности информации» включает:

описание способов реализации (возникновения) угроз безопасности информации, которые могут быть использованы нарушителями разных видов и категорий;

описание интерфейсов объектов воздействия, доступных для использования нарушителями способов реализации угроз безопасности информации.

К модели угроз безопасности информации может прилагаться схема с отображением типов логических, физических интерфейсов объектов воздействия, в том числе требующих физического доступа к ним, а также соответствующие им способы реализации угроз безопасности информации.

7. Актуальные угрозы безопасности информации

Раздел «Актуальные угрозы безопасности информации» включает:

перечень возможных (вероятных) угроз безопасности информации для соответствующих способов их реализации и уровней возможностей нарушителей;

описание возможных сценариев реализации угроз безопасности информации;

выводы об актуальности угроз безопасности информации.

К модели угроз безопасности информации может прилагаться схема с отображением сценариев реализации угроз безопасности информации.[1]

[1] Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021).