ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК РОССИИ)

Утвержден ФСТЭК России

« » _____ 2015 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА
ОПРЕДЕЛЕНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
В ИНФОРМАЦИОННЫХ СИСТЕМАХ

ПРОЕКТ

2015

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий методический документ ФСТЭК России «Методика определения угроз безопасности информации в информационных системах» (далее – Методика) разработан и утвержден 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. № 1085.

Документ устанавливает единый методический подход к определению угроз безопасности информации и разработке моделей угроз безопасности информации в государственных информационных системах (далее – информационные системы), защита информации в которых обеспечивается в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17 (зарегистрирован Минюстом России 31 мая 2013 г., рег. № 28608).

По решению оператора персональных данных Методика может применяться для определения в соответствии с пунктом 1 части 2 статьи 19 Федерального закона «О персональных данных» угроз безопасности персональных данных при их обработке в информационных системах персональных данных, защита которых обеспечивается в соответствии с Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18 февраля 2013 г. № 21 (зарегистрирован Минюстом России 14 мая 2013 г., рег. № 28375).

Методика не распространяется на определение угроз безопасности информации, составляющей государственную тайну.

Методика предназначена для:

органов государственной власти, органов местного самоуправления и организаций, являющихся в соответствии с законодательством Российской Федерации обладателями информации, заказчиками и (или) операторами информационных систем;

организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по созданию (проектированию) информационных систем;

организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по защите информации в ходе создания (проектирования) и эксплуатации информационных систем;

организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по аттестации (оценке соответствия) информационных систем требованиям о защите информации.

Настоящая Методика применяется на этапах создания информационных систем для определения и оценки угроз безопасности информации и разработки моделей угроз, а также в ходе эксплуатации информационных систем при периодическом пересмотре (переоценке) угроз безопасности информации.

Методика применяется совместно с банком данных угроз безопасности информации, сформированным ФСТЭК России (ubi.fstec.ru), а также базовыми и типовыми моделями угроз безопасности информации в информационных системах различных классов и типов, разрабатываемых 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. № 1085.

Методика ориентирована на определение и оценку антропогенных угроз безопасности информации, возникновение которых обусловлено объективными факторами. Вместе с тем, часть приведенных в Методике подходов может также применяться для оценки техногенных угроз в случае, если они позволяют достичь целей такой оценки. Определение угроз, связанных со стихийными бедствиями и природными явлениями осуществляется в соответствии с правилами, установленными уполномоченными федеральными органами исполнительной власти, национальными стандартами и находятся за рамками настоящей Методики.

В случае, если в соответствии с настоящей Методикой к числу актуальных угроз, отнесены угрозы, связанные с утечкой информации по техническим каналам, дальнейшая их оценка проводится в соответствии со специальными требованиями и рекомендациями по технической защите конфиденциальной информации и методиками оценки защищенности конфиденциальной информации.

В Методике используются термины и их определения, установленные национальными стандартами в области защиты информации.

В связи с утверждением настоящего методического документа не применяется для определения угроз безопасности информации Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ФСТЭК России, 2008 г.).

2. ПРОЦЕСС ОПРЕДЕЛЕНИЯ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Целью определения угроз безопасности информации является установление того, существует ли возможность нарушения конфиденциальности, целостности или доступности информации, содержащейся в информационной системе, и приведет ли нарушение хотя бы одного из указанных свойств безопасности информации к наступлению неприемлемых негативных последствий (ущерба) для обладателя информации или оператора, а в случае обработки персональных данных и для субъектов персональных данных.

Определение угроз безопасности информации должно носить систематический характер и осуществляться как на этапе создания информационной системы и формирования требований по ее защите, так и в ходе эксплуатации информационной системы. Систематический подход к определению угроз безопасности информации необходим для того, чтобы определить потребности в конкретных требованиях к защите информации и создать адекватную эффективную систему защиты информации в информационной системе. Меры защиты информации, принимаемые обладателем информации и оператором, должны обеспечивать эффективное и своевременное выявление и блокирование (нейтрализацию) угроз безопасности информации, в результате реализации которых возможно наступление неприемлемых негативных последствий (ущерба).

Систематический подход к определению угроз безопасности информации предусматривает реализацию непрерывного процесса, в рамках которого определяется область применения процесса определения угроз, идентифицируются источники угроз и угрозы безопасности информации, оценивается возможность реализации угроз безопасности информации и степень возможного ущерба в случае такой реализации, осуществляется мониторинг (периодический пересмотр) и переоценка угроз безопасности информации.

Оценка угроз безопасности информации проводится экспертным методом. Рекомендации по формированию экспертной группы и проведению экспертной оценки при определении угроз безопасности информации приведены в приложении № 1 к настоящей Методике.

а) область применения процесса определения угроз безопасности информации

На этапах принятия решения о необходимости защиты информации в информационной системе и разработки требований к защите информации должны быть определены физические и логические границы информационной системы, в которых принимаются и контролируются меры защиты информации, за которые ответственен оператор, а также определены объекты защиты и сегменты информационной системы.

Процесс определения угроз безопасности информации должен охватывать все объекты защиты и сегменты в логических и физических границах информационной системы, в которых оператором принимаются и контролируются меры

защиты информации. Процесс определения угроз безопасности информации организуется подразделением оператора, назначенным ответственным за защиту информации в информационной системе. В случае, если информационная система имеет сегменты, эксплуатируемые разными подразделениями оператора, которые могут самостоятельно принимать и контролировать меры защиты информации, должны быть определены границы ответственности этих подразделений и порядок их взаимодействия в процессе определения угроз безопасности информации.

Область применения процесса определения угроз безопасности информации отражается в модели угроз безопасности информации наряду с областью действия модели угроз, структурно-функциональными характеристиками информационной системы и особенностями ее функционирования.

б) идентификация источников угроз и угроз безопасности информации

В обобщенном виде угрозы безопасности информации характеризуется источниками угроз, факторами, обуславливающими возможность реализации угроз, способами (методами) реализации угроз и последствиями от реализации угроз безопасности информации.

Важным этапом в процессе определения угроз безопасности информации является идентификация лиц или событий (явлений), в результате действий (наступления, возникновения) которых возможно нарушение конфиденциальности, целостности или доступности информации, содержащейся в информационной системе, и возникновение неприемлемых негативных последствий (ущерба).

В качестве источников угроз безопасности информации могут выступать субъекты (физические лица, организации, государства) или явления (техногенные аварии, стихийные бедствия, иные природные явления).

Источники угроз безопасности информации являются определяющим фактором при определении угроз безопасности информации в информационных системах. В процессе определения угроз безопасности информации подлежат оценке те угрозы, у которых есть источники и источники имеют возможности и условия для реализации угроз безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями ее функционирования.

Источники угроз безопасности информации могут быть следующих типов:

антропогенные источники (антропогенные угрозы);

техногенные источники (техногенные угрозы);

стихийные источники (угрозы стихийных бедствий, иных природных явлений).

В качестве источников антропогенных угроз безопасности информации могут выступать:

лица, осуществляющие преднамеренные действия с целью доступа к информации (воздействия на информацию), содержащейся в информационной системе, или нарушения функционирования информационной системы или обслу-

живающей ее инфраструктуры (преднамеренные угрозы безопасности информации);

лица, имеющие доступ к информационной системе, не преднамеренные действия которых могут привести к нарушению безопасности информации (непреднамеренные угрозы безопасности информации).

Для информационных систем, в которых целью защиты является обеспечение целостности и доступности обрабатываемой информации, в обязательном порядке подлежат оценке техногенные угрозы, связанные с отказами или сбоями в работе технических средств или программного обеспечения. Такие угрозы могут быть обусловлены:

низким качеством (надежностью) технических, программных или программно-технических средств;

низким качеством (надежностью) сетей связи и (или) услуг связи;

отсутствием или низкой эффективностью систем резервирования или дублирования программно-технических и технических средств;

низким качеством (надежностью) инженерных систем (кондиционирования, электроснабжения, охранных систем и т.д.);

низким качеством обслуживания со стороны обслуживающих организаций и лиц.

При определении угроз безопасности информации оценке подлежат угрозы, связанные со всеми типами источников. Однако в целях создания и эксплуатации адекватной эффективной системы защиты информации в информационной системе следует, в первую очередь, уделять внимание оценке антропогенных угроз, связанных с несанкционированными (неправомерными) действиями субъектов по нарушению безопасности (конфиденциальности, целостности, доступности) информации, в том числе целенаправленными воздействиями программными (программно-техническими) средствами на информационные системы, осуществляемые в целях нарушения (прекращения) их функционирования (компьютерные атаки).

Также при определении угроз безопасности информации наряду с угрозами, реализация которых может привести непосредственно к нарушению конфиденциальности, целостности или доступности информации (прямыми угрозами), необходимо выявлять и оценивать угрозы, создающие условия для реализации прямых угроз безопасности информации (косвенные угрозы). В качестве косвенных угроз безопасности информации могут рассматриваться угрозы повышения привилегий, исчерпания вычислительных ресурсов, недоступности обновления программного обеспечения и иные угрозы безопасности информации.

В процессе определения угроз безопасности информации на всех стадиях (этапах) жизненного цикла информационных систем необходимо регулярно проводить идентификацию источников угроз, оценивать их возможности и определять на этой основе угрозы безопасности информации. Данные о нарушителях и их возможностях по реализации угроз безопасности информации, полученные при идентификации источников угроз, включаются в модели угроз безопасности информации.

Для идентификации угроз безопасности информации в информационной системе определяются:

возможности (тип, вид, потенциал) нарушителей, необходимые им для реализации угроз безопасности информации;

уязвимости, которые могут использоваться при реализации угроз безопасности информации (включая специально внедренные программные закладки);

способы (методы) реализации угроз безопасности информации;

объекты информационной системы, на которые направлена угроза безопасности информации (объекты воздействия);

результат и последствия от реализации угроз безопасности информации.

Каждая угроза безопасности информации в информационной системе описывается (идентифицируется) следующим образом:

$УБИ_j$ = [нарушитель (источник угрозы); уязвимости; способы реализации угрозы; объекты воздействия; последствия от реализации угрозы].

в) оценка вероятности (возможности) реализации угроз безопасности информации и степени возможного ущерба

Идентифицированная угроза безопасности информации подлежит нейтрализации (блокированию), если она является актуальной ($УБИ_j^A$) для информационной системы, то есть в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования существует вероятность (возможность) реализации рассматриваемой угрозы нарушителем с соответствующим потенциалом и ее реализация приведет к неприемлемым негативным последствиям (ущербу):

$УБИ_j^A$ = [вероятность (возможность) реализации угрозы (P_j); степень ущерба (X_j)].

Актуальные угрозы безопасности информации включаются в модель угроз безопасности информации. Модель угроз безопасности информации, учитывая особенности информационной системы, используемые в ней программные, программно-технические, технические средства и процессы обработки информации, дает описание угроз безопасности, которым подвержена информационная система. Структура модели угроз безопасности информации приведена в приложении № 2 к настоящей Методике.

г) мониторинг и переоценка угроз безопасности информации

Определение угроз безопасности информации на этапе создания информационной системы позволяет обеспечить формирование требований и внедрение эффективной адекватной системы защиты информации в информационной системе для угроз, актуальных к моменту ввода в эксплуатацию информационной системы.

В ходе эксплуатации информационной системы оператор, обеспечивая достижение целей и задач информационной системы, может изменять ее базовую конфигурацию, что приводит к изменению структурно-функциональных характеристик информационной системы и применяемых информационных технологий. Также в процессе эксплуатации возможно изменение состава и значимости обрабатываемой информации и особенностей функционирования информационной системы.

В этих условиях процесс определения угроз безопасности информации должен носить систематический характер. В ходе эксплуатации информационной системы регулярно проводится анализ изменения угроз безопасности информации, а актуальные угрозы безопасности информации подлежат периодической переоценке. Периодичность переоценки определяется организацией исходя из особенностей функционирования информационной системы. Рекомендуется пересматривать угрозы безопасности информации не реже одного раза в год. По результатам анализа проводится уточнение (при необходимости) модели угроз безопасности информации.

Пересмотр (переоценка) угроз безопасности информации, как минимум, осуществляется в случаях:

изменения требований законодательства Российской Федерации о защите информации, нормативных правовых актов и методических документов, регламентирующих защиту информации;

изменения конфигурации (состава основных компонентов) и особенностей функционирования информационной системы, следствием которых стало возникновение новых угроз безопасности информации;

выявления уязвимостей, приводящих к возникновению новых угроз безопасности информации или к повышению возможности реализации существующих;

появления сведений и фактов о новых возможностях нарушителей.

3. ОЦЕНКА ВОЗМОЖНОСТЕЙ НАРУШИТЕЛЕЙ ПО РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ (РАЗРАБОТКА МОДЕЛИ НАРУШИТЕЛЯ)

Целью оценки возможностей нарушителей по реализации угроз безопасности информации является формирование предположения о типах, видах нарушителей, которые могут реализовать угрозы безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования, а также потенциале этих нарушителей и возможных способах реализации угроз безопасности информации.

Результаты оценки возможностей нарушителей включаются в модель нарушителя, которая является составной частью (разделом) модели угроз безопасности информации и содержит:

типы, виды и потенциал нарушителей, которые могут обеспечить реализацию угроз безопасности информации;

цели, которые могут преследовать нарушители каждого вида при реализации угроз безопасности информации;

возможные способы реализации угроз безопасности информации.

а) типы нарушителей

Типы нарушителей определяются по результатам анализа прав доступа субъектов к информации и (или) к компонентам информационной системы, а также анализа возможностей нарушителей по доступу к компонентам информационной системы исходя из структурно-функциональных характеристик и особенностей функционирования информационной системы.

В зависимости от имеющихся прав доступа нарушители могут иметь легитимный физический (непосредственный) и (или) логический доступ к компонентам информационной системы и (или) содержащейся в них информации или не иметь такого доступа.

Анализ прав доступа проводится, как минимум, в отношении следующих компонент информационной системы:

устройств ввода/вывода (отображения) информации;

беспроводных устройств;

программных, программно-технических и технических средств обработки информации;

съемных машинных носителей информации;

машинных носителей информации, выведенных из эксплуатации;

активного (коммутационного) и пассивного оборудования каналов связи;

каналов связи, выходящих за пределы контролируемой зоны.

С учетом наличия прав доступа и возможностей по доступу к информации и (или) к компонентам информационной системы нарушители подразделяются на два типа:

внешние нарушители (тип I) – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы;

внутренние нарушители (тип II) – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам.

Наибольшими возможностями по реализации угроз безопасности обладают внутренние нарушители. При оценке возможностей внутренних нарушителей необходимо учитывать принимаемые оператором организационные меры по допуску субъектов к работе в информационной системе. Возможности внутреннего нарушителя существенным образом зависят от установленного порядка допуска физических лиц к информационной системе и ее компонентам, а также мер по контролю за доступом и работой этих лиц.

Внешнего нарушителя необходимо рассматривать в качестве актуального во всех случаях, когда имеются подключения информационной системы к внешним информационно-телекоммуникационным сетям и (или) имеются линии связи, выходящие за пределы контролируемой зоны, используемые для иных подключений.

б) виды и потенциал нарушителей

Угрозы безопасности информации в информационной системе могут быть реализованы следующими видами нарушителей:

специальные службы иностранных государств (блоков государств);

террористические, экстремистские группировки;

преступные группы (криминальные структуры);

внешние субъекты (физические лица);

конкурирующие организации;

разработчики, производители, поставщики программных, технических и программно-технических средств;

лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ;

лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.);

пользователи информационной системы;

администраторы информационной системы и администраторы безопасности;

бывшие работники (пользователи).

Виды нарушителей, характерных для информационной системы с заданными структурно-функциональными характеристиками и особенностями функционирования, определяются на основе предположений (прогноза) о возможных целях (мотивации) при реализации угроз безопасности информации этими нарушителями.

В качестве возможных целей (мотивации) реализации нарушителями угроз безопасности информации в информационной системе могут быть:

нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики;

реализация угроз безопасности информации по идеологическим или политическим мотивам;

организация террористического акта;

причинение имущественного ущерба путем мошенничества или иным преступным путем;

дискредитация или дестабилизация деятельности органов государственной власти, организаций;

получение конкурентных преимуществ;

внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки;

любопытство или желание самореализации;

выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды;

реализация угроз безопасности информации из мести;

реализация угроз безопасности информации непреднамеренно из-за неосторожности или неквалифицированных действий.

Предположения о целях (мотивации) нарушителей делаются с учетом целей и задач информационной системы, вида обрабатываемой информации, а также с учетом результатов оценки степени возможных последствий (ущерба) от нарушения конфиденциальности, целостности или доступности информации. Виды нарушителя и их возможные цели (мотивация) реализации угроз безопасности информации приведены в таблице 1.

Таблица 1

№ вида	Виды нарушителя	Типы нарушителя	Возможные цели (мотивация) реализации угроз безопасности информации
1	Специальные службы иностранных государств (блоков государств)	Внешний, внутренний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Дискредитация или дестабилизация деятельности органов государственной власти, организаций
2	Террористические, экстремистские группировки	Внешний	Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Совершение террористических актов. Идеологические или политические мотивы. Дестабилизация деятельности органов государственной вла-

			сти, организаций
3	Преступные группы (криминальные структуры)	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
4	Внешние субъекты (физические лица)	Внешний	Идеологические или политические мотивы. Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды
5	Конкурирующие организации	Внешний	Получение конкурентных преимуществ. Причинение имущественного ущерба путем обмана или злоупотребления доверием
6	Разработчики, производители, поставщики программных, технических и программно-технических средств	Внешний	Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия
7	Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия
8	Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора	Внутренний	Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифициро-

	(администрация, охрана, уборщики и т.д.)		ванные действия
9	Пользователи информационной системы	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
10	Администраторы информационной системы и администраторы безопасности	Внутренний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия
11	Бывшие работники (пользователи)	Внешний	Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия

При оценке возможностей нарушителей необходимо исходить из условий, что для повышения своих возможностей нарушители 1 вида могут вступать в сговор с нарушителями 3, 4, 6, 7, 8, 9 и 10 видов. Нарушители 2 вида могут вступать в сговор с нарушителями 4, 7, 8, 9 и 10 видов. Нарушители 3 вида могут вступать в сговор с нарушителями 4, 7, 8, 9 и 10 видов. В случае принятия таких предположений цели (мотивация) и возможности нарушителей подлежат объединению.

Возможности каждого вида нарушителя по реализации угроз безопасности информации характеризуются его потенциалом. Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности информации в информационной системе с заданными струк-

турно-функциональными характеристиками и особенностями функционирования.

В зависимости от потенциала, требуемого для реализации угроз безопасности информации, нарушители подразделяются на:

нарушителей, обладающих базовым (низким) потенциалом нападения при реализации угроз безопасности информации в информационной системе;

нарушителей, обладающих базовым повышенным (средним) потенциалом нападения при реализации угроз безопасности информации в информационной системе;

нарушителей, обладающих высоким потенциалом нападения при реализации угроз безопасности информации в информационной системе.

Потенциал нарушителей и их возможности приведены в таблице 2.

Таблица 2

№	Потенциал нарушителей	Виды нарушителей	Возможности по реализации угроз безопасности информации
1	Нарушители с базовым (низким) потенциалом	Внешние субъекты (физические лица), лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора, пользователи информационной системы, бывшие работники, лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных работ	Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему
2	Нарушители с базовым повышенным (средним) потенциалом	Террористические, экстремистские группировки, преступные группы (криминальные структу-	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных ком-

		ры), конкурирующие организации, разработчики, производители, поставщики программных, технических и программно-технических средств, администраторы информационной системы и администраторы безопасности	понент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы
3	Нарушители с высоким потенциалом	Специальные службы иностранных государств (блоков государств)	Обладают всеми возможностями нарушителей с базовым и базовым повышенным потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок. Имеют хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализиро-

			ванных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее. Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений

в) возможные способы реализации угроз безопасности информации

Целью определения возможных способов реализации угроз безопасности информации является формирование предположений о возможных сценариях реализации угроз безопасности информации, описывающих последовательность (алгоритмы) действий отдельных видов нарушителей или групп нарушителей и применяемые ими методы и средства для реализации угроз безопасности информации.

Возможные способы реализации угроз безопасности информации зависят от структурно-функциональных характеристик и особенностей функционирования информационной системы.

Угрозы безопасности информации могут быть реализованы нарушителями за счет:

несанкционированного доступа и (или) воздействия на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах));

несанкционированного доступа и (или) воздействия на объекты на общесистемном уровне (базовые системы ввода-вывода, гипервизоры, операционные системы);

несанкционированного доступа и (или) воздействия на объекты на прикладном уровне (системы управления базами данных, браузеры, web-приложения, иные прикладные программы общего и специального назначения);

несанкционированного доступа и (или) воздействия на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы);

несанкционированного физического доступа и (или) воздействия на линии, (каналы) связи, технические средства, машинные носители информации;

воздействия на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия).

Действия нарушителя в зависимости от его потенциала при реализации угроз безопасности информации предусматривают идентификацию и использование уязвимостей в микропрограммном, общесистемном и прикладном программном обеспечении, сетевом оборудовании, применяемых в информационной системе, а также в организации работ по защите информации и конфигурации информационной системы.

При определении способа реализации угроз безопасности информации необходимо учитывать то, что угрозы безопасности информации могут быть реализованы непосредственно за счет доступа к компонентам информационной системы и (или) информации или опосредовано (косвенно) за счет создания условий и (или) средств, обеспечивающих такой доступ, а также за счет доступа или воздействия на обслуживающую инфраструктуру, за которую оператор не отвечает. При этом локальной целью нарушителя, не имеющего доступа (прав доступа) к компонентам информационной системы и (или) информации, как правило, является получение доступа к информационной системе (в том числе через внешние сети связи общего пользования) и получение максимально возможных прав и привилегий при таком доступе.

Нарушители могут совершать действия, следствием которых является нарушение безопасности информации, преднамеренно (преднамеренные грозы безопасности информации) или случайно (непреднамеренные грозы безопасности информации).

Преднамеренные действия нарушителей могут заключаться в реализации целенаправленных или нецеленаправленных угроз безопасности информации.

Целенаправленная угроза безопасности информации направлена на интересующую нарушителя информационную систему с заранее известными ему структурно-функциональными характеристиками и особенностями функционирования. Целенаправленная угроза безопасности информации адаптирована к структурно-функциональным характеристикам информационной системы. При подготовке и реализации целенаправленных угроз безопасности информации нарушитель может использовать методы социальной инженерии, которые позволяют ему изучить поведение пользователей и их реакцию на поступающие к ним внешние данные.

Нецеленаправленная («веерная») угроза безопасности информации не ориентирована на конкретную информационную систему. Целями такой угрозы могут являться несанкционированный доступ, перехват управления или воздействие на как можно большее количество информационных систем. В данном случае нарушителю заранее не известны структурно-функциональные характеристики и условия функционирования информационной системы.

Реализация преднамеренных угроз безопасности информации, как правило, включает:

сбор информации об информационной системе, ее структурно-функциональных характеристиках, условиях функционирования;

выбор (разработка, приобретение) методов и средств, используемых для реализации угроз безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и условиями функционирования;

непосредственная реализация угроз безопасности информации в информационной системе (проникновение в информационную систему, закрепление в информационной системе, реализация неправомерных действий);

устранение признаков и следов неправомерных действий в информационной системе.

В зависимости от целей и потенциала нарушителя на каждом из этапов могут эксплуатироваться одна или несколько уязвимостей информационной системы.

При определении возможных способов реализации угроз безопасности информации необходимо исходить из следующих условий:

нарушитель может действовать один или в составе группы нарушителей;

в отношении информационной системы внешний нарушитель может действовать совместно с внутренним нарушителем;

угрозы могут быть реализованы в любое время и в любой точке информационной системы (на любом узле или хосте);

для достижения своей цели нарушитель выбирает наиболее слабое звено информационной системы.

Возможные способы реализации угроз безопасности информации, определенные на основе настоящего раздела, включаются в модель угроз безопасности информации.

4. ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Угроза безопасности информации является актуальной ($УБИ_j^A$), если для информационной системы с заданными структурно-функциональными характеристиками и особенностями функционирования существует вероятность реализации рассматриваемой угрозы нарушителем с соответствующим потенциалом и ее реализация приведет к неприемлемым негативным последствиям (ущербу) от нарушения конфиденциальности, целостности или доступности информации.

В качестве показателя актуальности угрозы безопасности информации ($УБИ_j^A$) принимается двухкомпонентный вектор, первый компонент которого характеризует вероятность реализации угрозы (P_j), а второй – степень возможного ущерба в случае ее реализации (X_j)

$$УБИ_j^A = [\text{вероятность реализации угрозы } (P_j); \text{ степень ущерба } (X_j)],$$

где P_j определятся на основе анализа статистических данных о частоте реализации угроз безопасности информации (возникновении инцидентов безопасности) в информационной системе и (или) однотипных информационных системах, а X_j определяется на основе оценок степени последствий от нарушения конфиденциальности, целостности или доступности информации.

При отсутствии статистических данных о реализации угроз безопасности информации (возникновении инцидентов безопасности) в информационной системе и (или) однотипных информационных системах, актуальность угрозы безопасности информации определяется на основе оценки возможности реализации угрозы безопасности информации (Y_j)

$$УБИ_j^A = [\text{возможность реализации угрозы } (Y_j); \text{ степень ущерба } (X_j)],$$

где Y_j определятся на основе оценки уровня защищенности информационной системы и потенциала нарушителя, требуемого для реализации угрозы безопасности. X_j также определяется на основе оценок степени последствий от нарушения конфиденциальности, целостности или доступности информации.

Актуальность угроз безопасности информации определяется в отношении угроз, для которых экспертным методом определено, что:

возможности (потенциал) нарушителя достаточны для реализации угрозы безопасности информации;

в информационной системе могут иметься потенциальные уязвимости, которые могут быть использованы при реализации j-ой угрозы безопасности информации;

структурно-функциональные характеристики и особенности функционирования информационной системы не исключают возможности применения способов, необходимых для реализации j-ой угрозы безопасности информации (существует сценарий реализации угрозы безопасности);

реализация угрозы безопасности информации приведет к нарушению конфиденциальности, целостности или доступности информации, в результате которого возможно возникновение неприемлемых негативных последствий (ущерба).

В качестве исходных данных об угрозах безопасности информации и их характеристиках используется банк данных угроз безопасности информации, сформированный и поддерживаемый ФСТЭК России, а также базовые и типовые модели угроз безопасности информации, разрабатываемые ФСТЭК России для различных классов и типов информационных систем.

Для определения угроз безопасности информации могут использоваться иные источники, в том числе опубликованные в общедоступных источниках данные об уязвимостях, компьютерных атаках, вредоносном программном обеспечении, а также результаты специально проведенных исследований по выявлению угроз безопасности информации. В этом случае потенциал нарушителя, возможные уязвимости, способы реализации угрозы безопасности информации и последствия от ее реализации определяются для каждой угрозы безопасности информации.

а) оценка вероятности (возможности) реализации угрозы безопасности информации

Под вероятностью реализации угрозы безопасности информации понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация j-ой угрозы безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования. Вводятся три вербальные градации этого показателя:

низкая вероятность – отсутствуют объективные предпосылки к реализации j-ой угрозы безопасности информации, отсутствует требуемая статистика по фактам реализации j-ой угрозы безопасности информации (возникновения инцидентов безопасности), отсутствует мотивация для реализации j-ой угрозы, возможная частота реализации j-ой угрозы не превышает 1 раза в 5 лет;

средняя вероятность – существуют предпосылки к реализации j-ой угрозы безопасности информации, зафиксированы случаи реализации j-ой угрозы безопасности информации (возникновения инцидентов безопасности) или имеется иная информация, указывающая на возможность реализации j-ой угрозы безопасности информации, существуют признаки наличия у нарушителя мотивации для реализации такой угрозы, возможная частота реализации j-ой угрозы не превышает 1 раза в год;

высокая вероятность – существуют объективные предпосылки к реализации j-ой угрозы безопасности информации, существует достоверная статистика реализации j-ой угрозы безопасности информации (возникновения инцидентов безопасности) или имеется иная информация, указывающая на высокую возможность реализации j-ой угрозы безопасности информации, у нарушителя имеются

мотивы для реализации j-ой угрозы, частота реализации j-ой угрозы – чаще 1 раза в год.

В случае отсутствия требуемых данных для оценки вероятности реализации угрозы безопасности информации или наличия сомнений в объективности экспертных оценок при определении вербальных градаций вероятности реализации угроз безопасности информации, актуальность j-ой угрозы безопасности информации определяется на основе оценки возможности ее реализации (Y_j).

Возможность реализации j-ой угрозы безопасности информации (Y_j) оценивается исходя из уровня защищенности информационной системы (Y_1) и потенциала нарушителя (Y_2), необходимого для реализации этой угрозы безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования:

Y_j = [уровень защищенности (Y_1); потенциал нарушителя (Y_2)].

При определении угроз безопасности информации на этапе создания информационной системы в случае, когда меры защиты информации не реализованы или не проведена оценка их достаточности и эффективности, оценка возможности реализации j-ой угрозы безопасности информации (Y_j) проводится относительно уровня проектной защищенности информационной системы ($Y_{1П}$):

Y_j = [уровень проектной защищенности ($Y_{1П}$); потенциал нарушителя (Y_2)].

Под уровнем проектной защищенности ($Y_{1П}$) понимается исходная защищенность информационной системы, обусловленная заданными при проектировании структурно-функциональными характеристиками и условиями ее функционирования. Уровень проектной защищенности ($Y_{1П}$) определяется на основе анализа проектных структурно-функциональных характеристик, приведенных в таблице 3.

Показатели, характеризующие проектную защищенность информационной системы

Таблица 3

Структурно-функциональные характеристики информационной системы, условия ее эксплуатации	Уровень проектной защищенности информационной системы ($Y_{1П}$)		
	Высокий	Средний	Низкий
1. По структуре информационной системы:			
автономное автоматизированное рабочее место;	+		
локальная информационная система;		+	
распределенная информационная система			+
2. По используемым информационным технологиям:			

системы на основе виртуализации;			+
системы, реализующие «облачные вычисления»;			+
системы с мобильными устройствами;			+
системы с технологиями беспроводного доступа;			+
грид-системы;			+
суперкомпьютерные системы		+	
3. По архитектуре информационной системы:			
системы на основе «тонкого клиента»;	+		
системы на основе одноранговой сети;		+	
файл-серверные системы;			+
центры обработки данных;			+
системы с удаленным доступом пользователей;			+
использование разных типов операционных систем (гетерогенность среды);		+	
использование прикладных программ, независимых от операционных систем;		+	
использование выделенных каналов связи		+	
4. По наличию (отсутствию) взаимосвязей с иными информационными системами:			
взаимодействующая с системами;			+
невзаимодействующая с системами		+	
5. По наличию (отсутствию) взаимосвязей (подключений) к сетям связи общего пользования:			
подключенная;			+
подключенная через выделенную инфраструктуру (gov.ru или иную);		+	
неподключенной	+		
6. По размещению технических средств:			
расположенные в пределах одной контролируемой зоны;	+		
расположенные в пределах нескольких контролируемых зон;		+	

расположенные вне контролируемой зоны			+
7. По режимам обработки информации в информационной системе: многопользовательский; однопользовательский	 +		 +
8. По режимам разграничения прав доступа: без разграничения; с разграничением		 +	 +
9. По режимам разделения функций по управлению информационной системой: без разделения; выделение рабочих мест для администрирования в отдельный домен; использование различных сетевых адресов; использование выделенных каналов для администрирования		 + + +	 +
10. По подходам к сегментированию информационной системы: без сегментирования; с сегментированием		 +	 +

В ходе создания информационной системы уровень ее проектной защищенности ($Y_{1П}$) определяется следующим образом:

а) информационная система имеет **высокий** уровень проектной защищенности ($Y_{1П}$), если не менее 80% характеристик информационной системы соответствуют уровню «высокий» (суммируются положительные решения по второму столбцу, соответствующему высокому уровню защищенности), а остальные - среднему уровню защищенности (положительные решения по третьему столбцу);

б) информационная система имеет **средний** уровень проектной защищенности ($Y_{1П}$), если не выполняются условия по пункту а) и не менее 90% характеристик информационной системы соответствуют уровню не ниже «средний» (берется отношение суммы положительных решений по третьему столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные - низкому уровню защищенности;

в) информационная система имеет **низкий** уровень проектной защищенности ($Y_{1П}$), если не выполняются условия по пунктам а) и б).

В соответствии с требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, до ввода в эксплуатацию информационной системы должны быть реализованы меры защиты информации, направленные на блокирование (нейтрализа-

цию) актуальных угроз безопасности информации. Таким образом, ввод в эксплуатацию информационной системы осуществляется при условии достижения высокого уровня исходной защищенности информационной системы от нарушителя с заданным потенциалом.

Вместе с тем, в ходе эксплуатации информационной системы возможно появление новых уязвимостей, повышение потенциала нарушителя, изменение структурно-функциональных характеристик, значимости обрабатываемой информации, особенностей функционирования информационной системы и других условий, приводящих к возникновению новых угроз безопасности информации, которые могут существенно снизить уровень проектной защищенности информационной системы. В этом случае для поддержания уровня защищенности информационной системы в ходе эксплуатации должен проводиться регулярный анализ изменения угроз безопасности информации, а актуальные угрозы безопасности информации подлежат периодической переоценке.

В ходе эксплуатации информационной системы уровень ее защищенности (Y_1) определяется следующим образом:

а) в информационной системе обеспечивается **высокий** уровень защищенности (Y_1), если в ходе эксплуатации информационной системы не появились дополнительные угрозы безопасности информации или в отношении появившихся дополнительных угроз безопасности информации с высокой оперативностью («за минуты») могут быть приняты меры защиты информации, нейтрализующие эти угрозы;

б) в информационной системе обеспечивается **средний** уровень защищенности (Y_1), если в ходе эксплуатации информационной системы появились дополнительные угрозы безопасности информации и в отношении них оперативно («за часы») могут быть приняты меры защиты информации, нейтрализующие эти угрозы;

в) в информационной системе обеспечивается **низкий** уровень защищенности (Y_1), если в ходе эксплуатации информационной системы появились дополнительные угрозы безопасности информации и в отношении них не могут быть с высокой оперативностью или оперативно приняты меры защиты информации, нейтрализующие эти угрозы.

Потенциал, требуемый нарушителю для реализации j-ой угрозы безопасности информации, может быть базовым (низким), базовым повышенным (средним) или высоким. Значение потенциала нарушителя (Y_2) для j-ой угрозы безопасности информации определяется на основе данных, приведенных в банке данных угроз безопасности информации ФСТЭК России, а также в базовых и типовых моделях угроз безопасности информации, разрабатываемых ФСТЭК России для информационных систем различных классов и типов. В случае отсутствия информации о потенциале нарушителя для реализации j-ой угрозы безопасности значение потенциала (Y_2) определяется в соответствии с приложением № 3 к настоящей Методике.

Возможность реализации j-ой угрозы безопасности информации (Y_j) в зависимости от уровня защищенности информационной системы ($Y_1/Y_{1П}$) и потен-

циала нарушителя (Y_2) определяется как высокая, средняя или низкая в соответствии с таблицей 4.

Возможность
реализации угрозы безопасности информации

Таблица 4

Уровень защищенности (Y_1/$Y_{1П}$) / Потенциал нарушителя (Y_2)	Высокий	Средний	Низкий
Базовый (низкий)	Низкая	Средняя	Высокая
Базовый повышенный (средний)	Средняя	Высокая	Высокая
Высокий	Высокая	Высокая	Высокая

б) оценка степени возможного ущерба от реализации угрозы безопасности информации

Для оценки степени возможного ущерба от реализации угрозы безопасности информации определяются возможный результат реализации угрозы безопасности информации в информационной системе, вид ущерба, к которому может привести реализация угрозы безопасности информации, степень последствий от реализации угрозы безопасности информации для каждого вида ущерба.

В качестве результата реализации угрозы безопасности информации рассматриваются непосредственное или опосредованное воздействие на конфиденциальность, целостность, доступность информации, содержащейся в информационной системе.

Непосредственное воздействие на конфиденциальность, целостность, доступность информации возможно в результате реализации прямой угрозы безопасности информации. В этом случае объектами воздействия угрозы являются непосредственно информация и (или) иные объекты защиты информационной системы или обеспечивающей инфраструктуры, которые обеспечивают получение, обработку, хранение, передачу, уничтожение информации в информационной системе, в результате доступа к которым или воздействия на которые возможно воздействие на конфиденциальность, целостность или доступность информации.

Опосредованное воздействие на конфиденциальность, целостность, доступность информации рассматривается в результате реализации косвенных угроз безопасности информации. Реализация косвенных угроз безопасности информации не приводит непосредственно к воздействию на конфиденциальность, целостность, доступность информации, но создает условия для реализации одной или нескольких прямых угроз безопасности информации, позволяющих реализовать такое воздействие. В этом случае в качестве результата реализации косвенной угрозы необходимо рассматривать результаты реализации всех пря-

мых угроз безопасности информации, которые возможно реализовать в случае реализации данной косвенной угрозы.

Результат реализации угрозы безопасности информации определяется воздействием угрозы на каждое свойство безопасности информации (конфиденциальность, целостность, доступность) в отдельности в соответствии с таблицей 5. При обработке в информационной системе двух и более видов информации (служебная тайна, персональные данные, налоговая тайна, иные установленные законодательством Российской Федерации виды информации) воздействие на конфиденциальность, целостность, доступность определяется отдельно для каждого вида информации (k, …, m), содержащейся в информационной системе.

Таблица 5

Свойство безопасности информации	Результат реализации угрозы безопасности информации	
	Не оказывает воздействия	Оказывает воздействие
Конфиденциальность $X_{k1}^{К}$	В результате реализации угрозы безопасности информации отсутствует возможность неправомерного доступа, копирования, предоставления или распространения информации	В результате реализации угрозы безопасности информации возможны неправомерный доступ, копирование, предоставление или распространение информации
Целостность $X_{k1}^{Ц}$	В результате реализации угрозы безопасности информации отсутствует возможность уничтожения или модифицирования информации	В результате реализации угрозы безопасности информации возможно уничтожение или модифицирование информации
Доступность $X_{k1}^{Д}$	В результате реализации угрозы безопасности информации отсутствует возможность блокирования информации	В результате реализации угрозы безопасности информации возможно блокирование информации

При определении степени возможного ущерба необходимо исходить из того, что в зависимости от целей и задач, решаемых информационной системой, видов обрабатываемой информации, воздействие на конфиденциальность, целостность или доступность каждого вида информации, содержащейся в информационной системе, может привести к различным видам ущерба. При этом для разных обладателей информации и операторов будут характерны разные виды ущерба.

Основные виды ущерба и возможные негативные последствия, к которым может привести нарушение конфиденциальности, целостности, доступности информации, приведены в таблице 6.

Таблица 6

Вид ущерба	Возможные негативнее последствия от нарушения конфиденциальности, целостности, доступности информации
Экономический (финансовый)	Снижение, как минимум, одного экономического показателя. Потеря (кража) финансовых средств. Недополучение ожидаемой (прогнозируемой) прибыли. Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. Потеря клиентов, поставщиков. Потеря конкурентного преимущества. Невозможность заключения договоров, соглашений. Другие прямые или косвенные финансовые потери
Социальный	Создание предпосылок для нанесения вреда здоровью граждан. Возможность нарушения функционирования объектов обеспечения жизнедеятельности граждан. Организация пикетов, забастовок, митингов и других акций. Увольнения. Увеличение количества жалоб в органы государственной власти или органы местного самоуправления. Появление негативных публикаций в общедоступных источниках. Невозможность (прерывание) предоставления социальных услуг (сервисов). Другие последствия, приводящие к нарастанию социальной напряженности в обществе
Политический	Создание предпосылок к обострению отношений в международных отношениях. Срыв двусторонних (многосторонних) контактов с зарубежными партнерами. Неспособность выполнения международных (двусторонних) договорных обязательств.

	Невозможность заключения международных (двусторонних) договоров, соглашений. Создание предпосылок к внутриполитическому кризису. Нарушение выборного процесса. Другие последствия во внутриполитической и внешнеполитической областях деятельности
Репутационный	Нарушение законодательных и подзаконных актов. Нарушение деловой репутации. Снижение престижа. Дискредитация работников. Утрата доверия. Неспособность выполнения договорных обязательств. Другие последствия, приводящие к нарушению репутации
Ущерб в области обороны, безопасности и правопорядка	Создание предпосылок к наступлению негативных последствий для обороны, безопасности и правопорядка. Нарушение общественного правопорядка. Неблагоприятное влияние на обеспечение общественного правопорядка. Возможность потери или снижения уровня контроля за общественным правопорядком. Отсутствие возможности оперативного оповещения населения о чрезвычайной ситуации. Другие последствия, приводящие к ущербу в области обороны, безопасности и правопорядка
Ущерб субъекту персональных данных	Создание угрозы личной безопасности. Финансовые или иные материальные потери физического лица. Вторжение в частную жизнь. Создание угрозы здоровью. Моральный вред. Утрата репутации. Другие последствия, приводящие к нарушению прав субъекта персональных данных
Технологический	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций). Принятие неправильных решений. Простой информационной системы или сегмента информационной системы Другие последствия, приводящие к нарушению технологии обработки информации

Указанные виды ущерба могут дополняться другими видами в зависимости от целей и задач, решаемых информационной системой, а также вида обрабатываемой в ней информации.

Степень возможного ущерба от реализации угрозы безопасности информации определяется степенью негативных последствий от нарушения конфиденциальности, целостности или доступности каждого вида информации, содержащейся в информационной системе.

Степень негативных последствий от нарушения конфиденциальности, целостности или доступности информации определяется для каждого вида ущерба, зависит от целей и задач, решаемых информационной системой, и может иметь разные значения для разных обладателей информации и операторов. В качестве единой шкалы измерения степени негативных последствий принимаются значения «незначительные», «умеренные» и «существенные» негативные последствия. Каждым оператором определяется в указанной единой шкале измерений степень негативных последствий от нарушения конфиденциальности, целостности или доступности информации применительно ко всем целям и задачам, решаемым информационной системой.

Степень возможного ущерба определяется экспертным методом в соответствии с таблицей 7.

Таблица 7

Степень ущерба	Характеристика степени ущерба
Высокая	В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны существенные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять возложенные на них функции
Средняя	В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны умеренные негативные последствия. Информационная система и (или) оператор (обладатель информации) не могут выполнять хотя бы одну из возложенных на них функций
Низкая	В результате нарушения одного из свойств безопасности информации (конфиденциальности, целостности, доступности) возможны незначительные негативные последствия. Информационная система и (или) оператор (обладатель информации) могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств

При обработке в информационной системе двух и более видов информации (служебная тайна, персональные данные, налоговая тайна и иные установленные законодательством Российской Федерации виды информации) степень возможного ущерба определяется отдельно для каждого вида информации (k, …, m), обрабатываемой в информационной системе, применительно к каждому виду ущерба. Итоговая степень возможного ущерба устанавливается по наивысшим значениям степени возможного ущерба, определенным для конфиденциальности, целостности, доступности информации каждого вида информации применительно к каждому виду ущерба.

$$X_k = \max_i (X_k^i); i = К, Ц, Д.$$

в) **определение актуальности угрозы безопасности информации**

Решение об актуальности угрозы безопасности информации $УБИ_j^A$ для информационной системы с заданными структурно-функциональными характеристиками и условиями функционирования принимается в соответствии с таблицей 8.

Таблица 8

Вероятность (возможность) реализации угрозы (Y_i)	Степень возможного ущерба (X_j)		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная

Приложение № 1 к
Методике определения угроз безопасности
информации в информационных системах

Рекомендации по формированию экспертной группы и проведению экспертной оценки при определении угроз безопасности информации

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

Независимо от результата формирования экспертной группы при оценке угроз безопасности информации существуют субъективные факторы, связанные с психологией принятия решений человеком. Это также может приводить как к занижению (ослаблению), так и к завышению (усилению) экспертами прогнозов и предположений при определении 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 определении 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 определения угроз безопасности информации рекомендуется включать экспертов (независимо от того, реализуются ли функции обладателя информации, заказчика и оператора в рамках одной или нескольких организаций):

от подразделений обладателей информации, содержащейся в информационной системе;

от подразделений оператора информационной системы;

от подразделения по защите информации;

от лиц, предоставляющих услуги по обработке информации;

от разработчика информационной системы;

от операторов взаимодействующих внешних информационных систем (по согласованию).

В качестве экспертов рекомендуется привлекать специалистов, деятельность которых связана с обработкой информации в информационной системе, а

также специалистов, имеющие квалификацию и опыт работы в области применения информационных технологий и (или) в области защиты информации.

При привлечении в качестве экспертов специалистов от подразделений по защите информации рекомендуется привлекать лиц, имеющих высшее образование или прошедших переподготовку (повышение квалификации) по направлению подготовки «Информационная безопасность», или имеющих не менее трех лет стажа практической работы в своей сфере деятельности.

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.

Состав экспертной группы зависит от целей и задач информационной системы, но не должен быть меньше 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, как минимум, следующих параметров:

цели реализации угроз безопасности информации (мотивация нарушителей);

типы и виды нарушителей;

уязвимости, которые могут быть использованы для реализации угроз безопасности информации;

способы реализации угроз безопасности информации;

степень воздействия угрозы безопасности информации на каждое из свойств безопасности информации;

последствия от реализации угроз безопасности информации;

вероятность реализации угроз безопасности информации;

уровень защищенности информационной системы;

потенциал нарушителя, требуемый для реализации угрозы безопасности информации (в случае отсутствия потенциала в банке данных 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 мене двух раундов оценки), результаты которой заносятся в таблицу 1.1;

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

Таблица 1.1

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

Приложение № 2 к
Методике определения угроз безопасности
информации в информационных системах

Структура модели угроз безопасности информации

Модель угроз безопасности информации содержит следующие разделы:

1. Общие положения.

2. Описание информационной системы и особенностей ее функционирования.

2.1. Цель и задачи, решаемые информационной системой.

2.2. Описание структурно-функциональных характеристик информационной системы.

2.3. Описание технологии обработки информации.

3. Возможности нарушителей (модель нарушителя).

3.1. Типы и виды нарушителей.

3.2. Возможные цели и потенциал нарушителей.

3.3. Возможные способы реализации угроз безопасности информации.

4. Актуальные угрозы безопасности информации.

Приложения (при необходимости).

Раздел «Общие положения» содержит назначение и область действия документа, информацию о полном наименовании информационной системы, для которой разработана модель угроз безопасности информации, а также информацию об использованных для разработки модели угроз безопасности информации нормативных и методических документах, национальных стандартах. В данный раздел также включается информация об используемых данных и источниках, на основе которых определяются угрозы безопасности информации (документация, исходные тексты программ, опросы персонала, журналы регистрации средств защиты, отчеты об аудите и иные источники).

Раздел «Описание информационной системы и особенностей ее функционирования» содержит общую характеристику информационной системы, описание структурно-функциональных характеристик информационной системы, описание взаимосвязей между сегментами информационной системы, описание взаимосвязей с другими информационными системами и информационно-телекоммуникационными сетями, описание технологии обработки информации. Также в данном разделе приводятся предположения, касающиеся информационной системы и особенностей ее функционирования (в частности предположения об отсутствии неучтенных беспроводных каналов доступа или динамичность выделения адресов узлам информационной системы, иные предположения). В раздел включаются любые ограничения, касающиеся информационной системы и особенностей ее функционирования.

Раздел «Возможности нарушителей (модель нарушителя)» содержит описание типов, видов, потенциала и мотивации нарушителей, от которых необходимо обеспечить защиту информации в информационной системе, способов реа-

лизации угроз безопасности информации. В данный раздел также включаются предположения, касающиеся нарушителей (в частности предположение об отсутствии у нарушителя возможности доступа к оборудованию, сделанному на заказ и применяемому при реализации угрозы, предположение о наличии (отсутствии) сговора между внешними и внутренними нарушителями или иные предположения). В раздел включаются любые ограничения, касающиеся определения нарушителей (в частности исключение администраторов информационной системы или администраторов безопасности из числа потенциальных нарушителей или иные предположения).

Раздел «Актуальные угрозы безопасности информации» содержит описание актуальных угроз безопасности, включающее наименование угрозы безопасности информации, возможности нарушителя по реализации угрозы, используемые уязвимости информационной системы, описание способов реализации угрозы безопасности информации, объекты воздействия, возможные результат и последствия от реализации угрозы безопасности информации.

Приложение № 3 к
Методике определения угроз безопасности
информации в информационных системах

Определение потенциала нарушителя, необходимого для реализации угрозы безопасности информации в информационной системе

Настоящее приложение применяется для определения потенциала, необходимого для реализации угрозы безопасности информации, данные по которой отсутствуют в банке данных угроз безопасности информации, и характеристики которых определяются на основе иных источников или результатов исследований.

Приведенный подход к оценке потенциала нарушителя направлен на снижение уровня субъективности и неопределенности при оценке потенциала нарушителя, который требуется для реализации угрозы безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и особенностями функционирования.

Исходными данными для определения потенциала нарушителя являются:

данные об аппаратном, общесистемном и прикладном программном обеспечении, применяемых информационных технологиях, особенностях функционирования информационной системы;

данные об уязвимостях в аппаратном, общесистемном и прикладном программном обеспечении, опубликованные в различных базах данных уязвимостей, полученные в результате исследований (тестировании) или полученные от уполномоченных федеральных органов исполнительной власти и организаций.

При оценке потенциала нарушителя необходимо исходить из того, что для успешного достижения целей реализации угроз безопасности информации, нарушителю необходимо осуществить подготовку к реализации угрозы и непосредственно реализацию угрозы безопасности информации. При этом не единственным, но необходимым условием на этапе подготовки к реализации угрозы безопасности информации является идентификация уязвимостей в информационной системе, а на этапе реализации угрозы безопасности информации – использование уязвимостей информационной системы.

Таким образом, для определения потенциала нарушителя необходимо оценить возможности нарушителя идентифицировать уязвимости и использовать их в информационной системе в ходе подготовки к реализации и непосредственно в ходе реализации угрозы безопасности информации. Для проведения указанной оценки делается предположение о наличии уязвимостей, которые потенциально содержатся в информационной системе и могут быть использованы для реализации угрозы безопасности информации.

Потенциальные уязвимости определяются для каждого класса и типа программного обеспечения и для каждого узла (хоста) информационной системы исходя из условия, что для реализации угрозы безопасности информации нару-

шителю необходимо идентифицировать и использовать как минимум одну уязвимость на каждом узле и хосте.

В качестве исходных данных для определения потенциальных уязвимостей используются данные по составу информационной системы и особенностям ее функционирования, а также данные об уязвимостях в этом программном обеспечении, опубликованные в общедоступных источниках, полученные по результатам исследований и (или) полученные от уполномоченных органов и организаций.

Для каждой выявленной потенциальной уязвимости проводится оценка возможностей ее идентификации и использования в информационной системе нарушителем, обладающим определенными возможностями и для каждого из возможных сценариев реализации угрозы безопасности информации.

Оценка возможностей нарушителя по идентификации и использованию уязвимости в информационной системе проводится по результатам определения следующих показателей:

время, затрачиваемое нарушителем на идентификацию и использование уязвимости (затрачиваемое время);

техническая компетентность нарушителя;

знание нарушителем проекта и информационной системы;

оснащенность нарушителя;

возможности нарушителя по доступу к информационной системе.

Во многих случаях указанные показатели являются зависимыми и могут в различной степени заменять друг друга. В частности, показатели технической компетентности или оснащенности могут заменяться показателем затрачиваемого времени.

а) определение показателя «затрачиваемое время»

Показатель «затрачиваемое время» характеризует время, непрерывно затрачиваемое нарушителем для идентификации и использования уязвимости для реализации угрозы безопасности информации.

Показатель «затрачиваемое время» может принимать значения «за минуты», «за часы», «за дни» или «за месяцы».

Значение «за минуты» присваивается, если для реализации угрозы безопасности информации нарушитель затратит менее получаса на идентификацию и использование уязвимости.

Значение «за часы» присваивается, если для реализации угрозы безопасности информации нарушитель затратит менее чем один день на идентификацию и использование уязвимости.

Значение «за дни» присваивается, если для реализации угрозы безопасности информации нарушитель затратит менее чем один месяц на идентификацию и использование уязвимости.

Значение «за месяцы» присваивается, если для реализации угрозы безопасности информации нарушитель затратит, как минимум, месяц на идентификацию и использование уязвимости.

б) определение показателя «техническая компетентность нарушителя»

Показатель «техническая компетентность нарушителя» характеризует, каким уровнем знаний и подготовкой в области информационных технологий и защиты информации должен обладать нарушитель, чтобы идентифицировать и использовать уязвимости для реализации угрозы безопасности информации.

Показатель «техническая компетентность нарушителя» может принимать значения «специалист», «профессионал» или «непрофессионал».

Значение «профессионал» присваивается, если нарушитель имеет хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе, а также обладает специальными знаниями о методах и средствах выявления новых уязвимостей и способах реализации угроз безопасности информации для информационных систем данного типа.

Значение «специалист» присваивается, если нарушитель имеет осведомленность о мерах защиты информации, применяемых в информационной системе данного типа.

Значение «непрофессионал» присваивается, если нарушитель имеет слабую осведомленность (по сравнению со специалистами или профессионалами) о мерах защиты информации, применяемых в информационных системах данного типа, и не обладает специальными знаниями по реализации угроз безопасности информации.

в) определение показателя «знание нарушителем проекта и информационной системы»

Показатель «знание нарушителем проекта и информационной системы» характеризует, какие сведения об информационной системе и условиях ее эксплуатации доступны нарушителю, чтобы идентифицировать и использовать уязвимости для реализации угрозы безопасности информации.

Показатель «знание нарушителем проекта и информационной системы» может принимать значения «отсутствие знаний», «ограниченные знания» или «знание чувствительной информации».

Значение «отсутствие знаний» присваивается, если в результате принятия мер по защите информации нарушителю не может стать известно о структурно-функциональных характеристиках информационной системы, системе защиты информации информационной системы, а также об иной информации по разработке (проектированию) и эксплуатации информационной системы, включая сведения из конструкторской, проектной и эксплуатационной документации. При этом может быть доступна информация о целях и задачах, решаемых информационной системой. Данный показатель также присваивается, если сведения об информационной системе отнесены к информации ограниченного доступа и не могут быть доступны для неограниченного круга лиц.

Значение «ограниченные знания» присваивается, если нарушителю наряду с информацией о целях и задачах, решаемых информационной системой, может стать известна только эксплуатационная документация на информационную систему (в частности руководство пользователя и (или) правила эксплуатации информационной системы).

Значение «знание чувствительной информации» присваивается, если нарушителю может стать известны конструкторская (проектная) и эксплуатационная документация на информационную систему, информация о структурно-функциональных характеристиках информационной системы, системе защиты информационной системы.

г) определение показателя «возможности нарушителя по доступу к информационной системе»

Показатель «возможности нарушителя по доступу к информационной системе» характеризует, как долго по времени нарушитель должен иметь возможность доступа к информационной системе для идентификации и использования уязвимостей для реализации угроз безопасности информации.

Показатель «возможности нарушителя по доступу к информационной системе» может принимать значения «за минуты», «за часы», «за дни» или «за месяцы».

Значение «за минуты» присваивается, если для идентификации и использования уязвимости для реализации угрозы безопасности информации нарушителю требуется доступ менее получаса.

Значение «за часы» присваивается, если для идентификации и использования уязвимости для реализации угрозы безопасности информации нарушителю требуется доступ менее одного дня.

Значение «за дни» присваивается, если для идентификации и использования уязвимости для реализации угрозы безопасности информации нарушителю требуется доступ менее одного месяца.

Значение «за месяцы» присваивается, если для идентификации и использования уязвимости для реализации угрозы безопасности информации нарушителю требуется доступ более одного месяца.

Показатель «возможности нарушителя по доступу к информационной системе» взаимосвязан с показателем «затраченное время». Идентификация и использование уязвимости при реализации угрозы безопасности информации могут требовать продолжительного времени по доступу к информационной системе, что увеличивает возможность обнаружения уязвимости. В отдельных случаях продолжительный доступ к информационной системе не требуется (методы и средства реализации угроз безопасности разрабатываются автономно), но при этом требуется кратковременный доступ к информационной системе.

д) определение показателя «оснащенность нарушителя»

Показатель «оснащенность нарушителя» характеризует, какие программные и (или) программно-технические средства требуются нарушителю для идентификации и использования уязвимостей для реализации угроз безопасности информации.

Показатель «оснащенность нарушителя» может принимать значения «стандартное оборудование», «специализированное оборудование» или «оборудование, сделанное на заказ».

Значение «стандартное оборудование» присваивается, если для идентификации или использования уязвимостей при реализации угрозы безопасности информации требуются программные (программно-технические) средства, легко доступные для нарушителя. К таким средствам, в первую очередь, относятся программные средства непосредственно информационной системы (отладчик в операционной системе, средства разработки и иные), программные средства, которые могут быть легко получены (программы, имеющиеся в свободном доступе в сети Интернет) или имеются простые сценарии реализации угроз.

Значение «специализированное оборудование» присваивается, если для идентификации или использования уязвимостей при реализации угрозы безопасности информации требуются программные (программно-технические) средства, которые отсутствуют в свободном доступе, но могут быть приобретены нарушителем без значительных усилий. К таким средствам, в первую очередь, относятся программные (программно-технические) средства, которые имеются в продаже (анализаторы кода, анализаторы протоколов и иные) или требуется разработка более сложных программ и сценариев реализации угрозы. Оборудование может быть закуплено, либо, например, могут быть использованы компьютеры, объединенные через сеть Интернет (бот-сети).

Значение «оборудование, сделанное на заказ» присваивается, если для идентификации или использования уязвимостей при реализации угрозы безопасности информации требуются программные (программно-технические) средства, которые недоступны широкому кругу лиц, так как требуется их специальная разработка с привлечением исследовательских организаций, или распространение этих средств контролируется в соответствии с законодательством. К такому оборудованию также относится дорогостоящие средства или средства, сведения о которых относятся к информации ограниченного доступа.

С целью вычисления потенциала нарушителя определяются числовые значения указанных показателей в соответствии с таблицей 3.1.

Таблица 3.1

Показатель возможностей нарушителя		Значения при идентификации уязвимости	Значения при использовании уязвимости
Затрачиваемое время	< 0,5 час	0	0
	< 1 день	2	3
	< 1 месяц	3	5
	> 1 месяц	5	8
Техническая компетентность нарушителя	Непрофессионал	0	0
	Специалист	2	3
	Профессионал	5	4
Знание проекта и информационной системы	Отсутствие знаний	0	0
	Ограниченные знания	2	2
	Знание чувствительной информации	5	4
Возможность доступа к информационной системе	< 0,5 час или не обнаруживаемый доступ	0	0
	< 1 день	2	4
	< 1 месяц	3	6
	> 1 месяц	4	9
	Не возможно		
Оснащенность нарушителя	Отсутствует	0	0
	Стандартное оборудование	1	2
	Специализированное оборудование	3	4
	Оборудование, сделанное на заказ	5	6

Для конкретной потенциальной уязвимости может возникнуть необходимость определять показатели несколько раз для различных способов реализации угроз безопасности информации (попеременно использовать разные значения показателей компетентности в сочетании со значениями времени и оборудования). При этом следует выбирать наибольшее значение, полученное при каждом расчете показателей.

Полученные на основе таблицы 3.1 значения характеристик потенциала нарушителя суммируются. Полученная сумма значений характеристик соотносится с диапазонами значений, приведенных в таблице 3.2, в соответствии с которой определяется потенциал нарушителя, необходимый для реализации угрозы безопасности информации.

Таблица 3.2

Диапазон значений	Потенциал нарушителя
<10	Потенциал недостаточен для реализации угрозы безопасности
10-17	Базовый (низкий)
18-24	Базовый повышенный (средний)
>24	Высокий

Мотивация нарушителя для реализации угроз безопасности информации может быть базовой или повышенной. Мотивация нарушителя характеризует уровень устремлений нарушителя к информации, содержащейся в информационной системе, или информационной системе в целом. При определении потенциала нарушителя необходимо исходить, как минимум, из его базовой мотивации.

Потенциал нарушителя, требуемый для реализации угрозы безопасности информации, переходит на следующий уровень (от низкого к среднего или от среднего к высокому), если определено, что нарушитель имеет повышенную мотивацию реализации угроз безопасности по отношению к информационной системе.

Мотивация нарушителя определяется как повышенная, если:

а) имеются сведения (в том числе опубликованные в общедоступных источниках) об устремлениях нарушителей к конкретной информационной системе и (или) отдельным ее объектам защиты; например, если информация, обрабатываемая в информационной системе, является высоко ценной для нарушителя или для нарушителя является крайне приоритетным нанести ущерб оператору информационной системы;

б) имеется информация, полученная от уполномоченных федеральных органов исполнительной власти, о намерении нарушителя осуществить неправомерные действия в отношении информационной системы и (или) информации, содержащейся в этой информационной системе.