ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
5 февраля 2021 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕТОДИКА
ОЦЕНКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

МОСКВА
2021

В книге всего пронумеровано 83 страницы

СОДЕРЖАНИЕ

1. Общие положения

1.1. Настоящая Методика оценки угроз безопасности информации (далее – Методика) разработана 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.

1.2. Методика определяет порядок и содержание работ по определению угроз безопасности информации, реализация (возникновение) которых возможна в информационных системах, автоматизированных системах управления, информационно-телекоммуникационных сетях, информационно-телекоммуникационных инфраструктурах центров обработки данных и облачных инфраструктурах (далее – системы и сети), а также по разработке моделей угроз безопасности информации систем и сетей.

1.3. Методика применяется для определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях, отнесенных к государственным и муниципальным информационным системам, информационным системам персональных данных, значимым объектам критической информационной инфраструктуры Российской Федерации, информационным системам управления производством, используемым организациями оборонно-промышленного комплекса, автоматизированным системам управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

В иных случаях решение о применении настоящей Методики принимается обладателями информации или операторами систем и сетей.

1.4. В документе не рассматриваются методические подходы по оценке угроз безопасности информации, связанных с нарушением безопасности шифровальных (криптографических) средств защиты информации, а также угроз, связанных с техническими каналами утечки информации.

1.5. Методика ориентирована на оценку антропогенных угроз безопасности информации, возникновение которых обусловлено действиями нарушителей.

1.6. На основе настоящей Методики могут разрабатываться отраслевые (ведомственные, корпоративные) методики оценки угроз безопасности информации, которые учитывают особенности функционирования систем и сетей в соответствующей области деятельности. Разрабатываемые отраслевые (ведомственные, корпоративные) методики оценки угроз безопасности информации не должны противоречить положениям настоящей Методики.

1.7. В Методике используются термины и определения, приведенные в приложении 1 к настоящей Методике, а также термины и определения, установленные законодательством Российской Федерации и национальными

стандартами в области защиты информации и обеспечения информационной безопасности.

1.8. Положения настоящей Методики применяются для оценки угроз безопасности информации в системах и сетях, решение о создании или модернизации (развитии) которых принято после даты ее утверждения, а также в эксплуатируемых системах и сетях.

Модели угроз безопасности информации систем и сетей, разработанные и утвержденные до утверждения настоящей Методики, продолжают действовать и подлежат изменению в соответствии с настоящей Методикой при развитии (модернизации) соответствующих систем и сетей.

В связи с утверждением настоящего методического документа не применяются для оценки угроз безопасности информации Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (ФСТЭК России, 2008 г.) и Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (ФСТЭК России, 2007 г.).

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. № 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 настоящей Методикой, 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 настоящей Методике.

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).

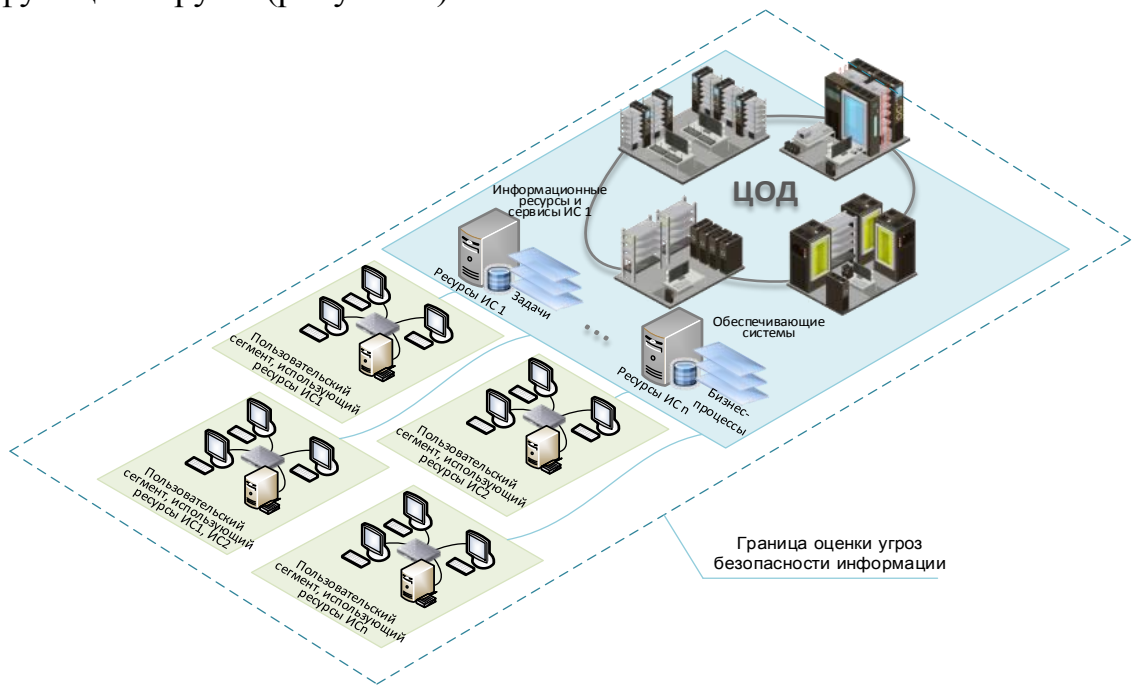

Рисунок 1. Оценка угроз безопасности информации в информационной инфраструктуре на базе центра обработки данных

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 настоящей Методике.

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 настоящей Методике.

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.

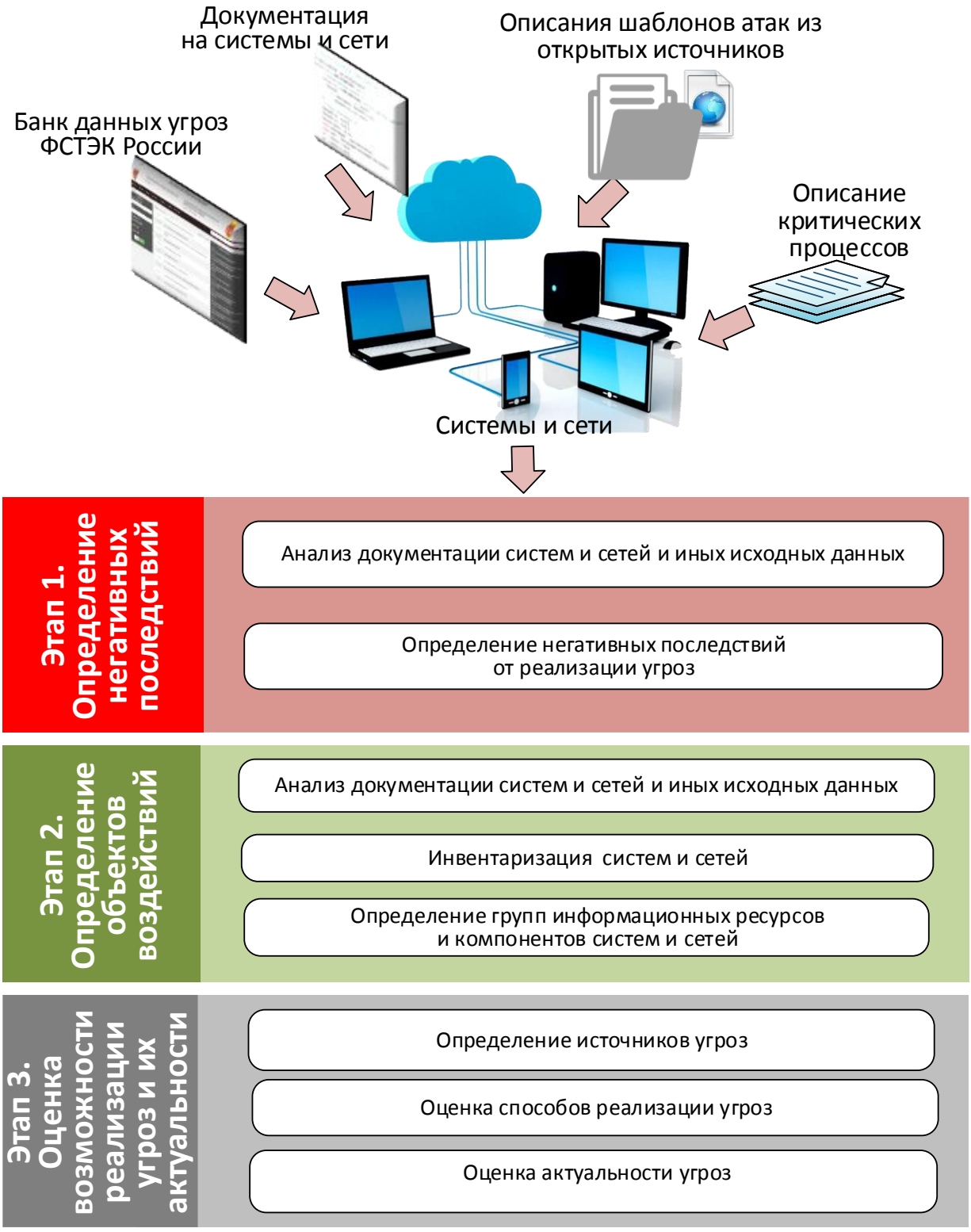

Рисунок 2. Общая схема проведения оценки угроз безопасности информации

3. Определение негативных последствий от реализации (возникновения) угроз безопасности информации

3.1. В ходе оценки угроз безопасности информации должны быть определены негативные последствия, которые могут наступить от реализации (возникновения) угроз безопасности информации.

3.2. Исходными данными для определения негативных последствий от реализации 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. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

б) 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;

в) документация на сети и системы (в части сведений о назначении и функциях систем и сетей, о составе и архитектуре систем и сетей);

г) технологические, производственные карты или иные документы, содержащие описание основных (критических) процессов (бизнес-процессов) обладателя информации, оператора;

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

Указанные исходные данные могут быть дополнены иными документами и сведениями с учетом особенностей области деятельности, в которой функционируют системы и сети.

3.3. На основе анализа исходных данных определяются событие или группа событий, наступление которых в результате реализации (возникновения) угроз безопасности информации может привести к:

а) нарушению прав граждан;

б) возникновению ущерба в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности государства;

в) возникновению финансовых, производственных, репутационных или иных рисков (видов ущерба) для обладателя информации, оператора.

Событие или группа событий определяются применительно к нарушению основных (критических) процессов (бизнес-процессов), выполнение которых обеспечивают системы и сети, и применительно к нарушению безопасности информации, содержащейся в системах и сетях.

3.4. В случае отсутствия у обладателя информации или оператора результатов оценки рисков (ущерба), возможные негативные последствия от реализации угроз безопасности информации могут определяться как на основе экспертной оценки специалистов, проводящих оценку угроз безопасности информации, так и на основе информации, представляемой профильными подразделениями или специалистами обладателя информации или оператора.

3.5. Определяемые в ходе оценки угроз безопасности информации негативные последствия должны быть конкретизированы применительно к областям и особенностям деятельности обладателя информации или оператора. Для систем и сетей обладателя информации или оператора может быть определено одно или несколько негативных последствий.

Пример 1: *1) если оператор обрабатывает персональные данные граждан, которые в соответствии с Федеральным законом «О персональных данных» подлежат обязательной защите, одним из возможных негативных последствий от реализации угроз безопасности информации является нарушение конфиденциальности персональных данных, в результате которого будут нарушены права субъектов персональных данных и соответствующие законодательные акты; 2) если оператор обеспечивает транспортировку нефти, одним из возможных негативных последствий от реализации угроз безопасности информации является разлив нефти из нефтепровода, повлекший наступление экологического ущерба; 3) если оператор предоставляет услуги связи, одним из возможных негативных последствий от реализации угроз безопасности информации является непредоставление услуг связи абонентам, повлекшее наступление ущерба в социальной сфере; 4) для оператора по переводу денежных средств одним из возможных негативных последствий от реализации угроз безопасности информации является хищение денежных средств, в результате которого возможны финансовые и репутационные риски.*

Виды рисков (ущербов) и типовые негативные последствия, которые могут наступить от реализации (возникновения) угроз безопасности информации, приведены в приложении 4 к настоящей Методике.

4. Определение возможных объектов воздействия угроз безопасности информации

4.1. В ходе оценки угроз безопасности информации должны быть определены информационные ресурсы и компоненты систем и сетей, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям – объекты воздействия.

Совокупность объектов воздействия и их интерфейсов определяет границы процесса оценки угроз безопасности информации и разработки модели угроз безопасности информации (рисунок 1, 3).

4.2. Исходными данными для определения возможных объектов воздействия являются:

а) общий перечень угроз безопасности информации, содержащейся 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. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

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

в) документация на сети и системы (в части сведений о составе и архитектуре, о группах пользователей и уровне их полномочий и типах доступа, внешних и внутренних интерфейсах);

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) негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с настоящей Методикой.

Указанные исходные данные могут быть дополнены иными документами и сведениями с учетом особенностей области деятельности, в которой функционируют системы и сети.

4.3. На основе анализа исходных данных и результатов инвентаризации систем и сетей определяются следующие группы информационных ресурсов и компонентов систем и сетей, которые могут являться объектами воздействия:

а) информация (данные), содержащаяся в системах и сетях (в том числе защищаемая информация, персональные данные, информация о конфигурации систем и сетей, данные телеметрии, сведения о событиях безопасности и др.);

б) программно-аппаратные средства обработки и хранения информации (в том числе автоматизированные рабочие места, серверы, включая промышленные, средства отображения информации, программируемые логические контроллеры, производственное, технологическое оборудование (исполнительные устройства));

в) программные средства (в том числе системное и прикладное программное обеспечение, включая серверы приложений, веб-приложений, системы управления базами данных, системы виртуализации);

г) машинные носители информации, содержащие как защищаемую информацию, так и аутентификационную информацию;

д) телекоммуникационное оборудование (в том числе программное обеспечение для управления телекоммуникационным оборудованием);

е) средства защиты информации (в том числе программное обеспечение для централизованного администрирования средств защиты информации);

ж) привилегированные и непривилегированные пользователи систем и сетей, а также интерфейсы взаимодействия с ними;

з) обеспечивающие системы.

Пример 2: *к основным информационным ресурсам и компонентам систем и сетей могут относиться системы хранения данных (базы данных), системы управления базами данных, веб-сайт, почтовый сервер, почтовый клиент, автоматизированное рабочее место пользователя, система управления и администрирования, контроллер домена, сетевые службы, проводные и беспроводные каналы передачи данных, телекоммуникационное оборудование и т.д.*

4.4. На этапе создания систем и сетей объекты воздействия определяются на основе предполагаемых архитектуры и условий функционирования систем и сетей, определенных на основе изучения и анализа исходных данных. В ходе эксплуатации систем и сетей, в том числе при развитии (модернизации) систем и сетей, объекты воздействия определяются для реальных архитектуры и условий функционирования систем и сетей, полученных по результатам анализа исходных данных и инвентаризации систем и сетей.

Инвентаризация систем и сетей проводится с использованием автоматизированных средств, которые позволяют определить компоненты систем и сетей, а также внешние и внутренние интерфейсы.

4.5. Для определенных информационных ресурсов и компонентов систем и сетей должны быть определены виды воздействия на них, которые могут привести к негативным последствиям. Основными видами таких воздействий являются:

а) утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности);

б) несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным;

в) отказ в обслуживании компонентов (нарушение доступности);

г) несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности);

д) несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач;

е) нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации.

4.6. Объекты воздействия определяются на аппаратном, системном и прикладном уровнях, на уровне сетевой модели взаимодействия, а также на уровне пользователей (рисунок 3).

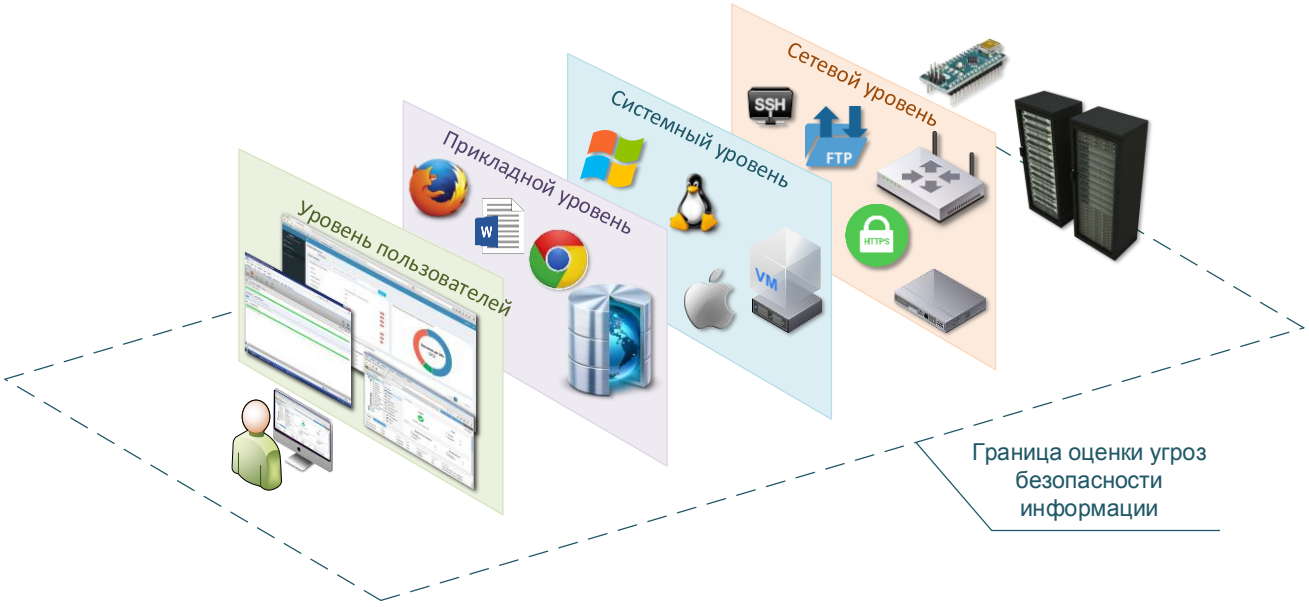

Рисунок 3. Уровни архитектуры систем и сетей, на которых определяются объекты воздействия

4.7. В процессе эксплуатации систем и сетей объекты воздействия и виды воздействия на них могут дополняться и изменяться относительно их состава и видов воздействия, определенных на этапе создания данных систем и сетей. В этом случае учет изменений должен проводиться в рамках реализации мероприятий по управлению конфигурацией систем и сетей и анализу угроз безопасности информации в ходе их эксплуатации.

4.8. При оценке угроз безопасности информации в системах и сетях, функционирующих на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, объекты воздействия определяются с учетом состава и содержания услуг,

предоставляемых поставщиком услуг (например, инфраструктура как услуга, платформа как сервис, программное обеспечение как сервис).

Арендуемые или используемые на ином законном основании программно-аппаратные средства и их интерфейсы, каналы связи, программное обеспечение (в том числе программное обеспечение виртуализации и построенных на его базе виртуальных машин, виртуальных серверов, систем управления виртуализацией, виртуальных каналов связи и т.д.) относятся к объектам воздействия, находящимся в границе оценки угроз безопасности информации оператора. В отношении остальной информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры угрозы безопасности информации оцениваются поставщиком услуг.

Пример распределения границ при оценке угроз безопасности информации между оператором и поставщиком услуг представлен на рисунке 4.

Рисунок 4. Пример распределения границ при оценке угроз безопасности информации в информационной инфраструктуре поставщика услуг

4.9. Объекты воздействия и виды воздействия на них должны быть конкретизированы применительно к архитектуре и условиям функционирования систем и сетей, а также областям и особенностям деятельности обладателя информации и оператора.

Пример 3: *1) разглашение персональных данных и (или) их модификация возможны в результате несанкционированного доступа к базе данных, в которой эта информация хранится; 2) разлив нефти из нефтепровода возможен в результате несанкционированного доступа к программируемому логическому контроллеру, обеспечивающему управление задвижками нефтепровода, и подмены хранящихся в нем значений уставок; 3) непредоставление услуг связи абонентам возможно в результате отказа в обслуживании маршрутизатора уровня ядра сети; 4) нарушение электроснабжения потребителей возможно в результате несанкционированного доступа к программируемому логическому контроллеру, управляющему выключателем, с целью подачи ложных команд на его отключение; 5) хищение денежных средств у оператора по переводу денежных средств возможно в результате подмены (модификации) информации, содержащейся в электронных сообщениях.*

Примеры определения объектов воздействия и видов воздействия на них приведены в приложении 5 к настоящей Методике.

5. Оценка возможности реализации (возникновения) угроз безопасности информации и определение их актуальности

5.1 Определение источников угроз безопасности информации

5.1.1. В ходе оценки угроз безопасности информации должны быть определены возможные антропогенные источники угроз безопасности информации, к которым относятся лица (группа лиц), осуществляющие реализацию угроз безопасности информации путем несанкционированного доступа и (или) воздействия на информационные ресурсы и (или) компоненты систем и сетей, – актуальные нарушители.

5.1.2. Исходными данными для определения возможных актуальных нарушителей 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. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

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

в) нормативные правовые акты Российской Федерации, в соответствии с которыми создается и функционирует система или сеть, содержащие описание назначения, задач (функций) систем и сетей, состав обрабатываемой информации и ее правовой режим;

г) документация на сети и системы (в части сведений 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);

д) договоры, соглашения или иные документы, содержащие условия использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (в части персонала поставщика услуг, имеющего доступ к этой инфраструктуре, его прав и обязанностей, уровня полномочий и типов доступа);

е) результаты оценки ущерба (рисков), проведенной обладателем информации или оператором;

ж) негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с настоящей Методикой;

з) объекты воздействия угроз безопасности информации и виды воздействия на них, определенные в соответствии с настоящей Методикой.

Указанные исходные данные могут быть дополнены иными документами и сведениями с учетом особенностей области деятельности, в которой функционируют системы и сети.

5.1.3. На основе анализа исходных данных, а также результатов оценки возможных целей реализации нарушителями угроз безопасности информации определяются виды нарушителей, актуальных для систем и сетей.

Основными видами нарушителей, подлежащих оценке, являются:

специальные службы иностранных государств;

террористические, экстремистские группировки;

преступные группы (криминальные структуры);

отдельные физические лица (хакеры);

конкурирующие организации;

разработчики программных, программно-аппаратных средств;

лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;

поставщики услуг связи, вычислительных услуг;

лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;

лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.);

авторизованные пользователи систем и сетей;

системные администраторы и администраторы безопасности;

бывшие (уволенные) работники (пользователи).

Указанные виды нарушителей могут быть дополнены иными нарушителями с учетом особенностей области деятельности, в которой функционируют системы и сети. Для одной системы и сети актуальными могут являться нарушители нескольких видов.

5.1.4. Нарушители признаются актуальными для систем и сетей, когда возможные цели реализации ими угроз безопасности информации могут привести к определенным для систем и сетей негативным последствиям и соответствующим рискам (видам ущерба). Возможные цели реализации угроз безопасности информации нарушителями приведены в приложении 6 к настоящей Методике.

Пример соответствия нарушителей, возможных целей реализации ими угроз безопасности информации и возможных негативных последствий и видов рисков (ущерба) от их реализации (возникновения) приведен в приложении 7 к настоящей Методике.

5.1.5. Нарушители имеют разные уровни компетентности, оснащенности ресурсами и мотивации для реализации угроз безопасности информации. Совокупность данных характеристик определяет уровень возможностей нарушителей по реализации угроз безопасности информации.

В зависимости от уровня возможностей нарушители подразделяются на нарушителей, обладающих:

базовыми возможностями по реализации угроз безопасности информации (H1);

базовыми повышенными возможностями по реализации угроз безопасности информации (H2);

средними возможностями по реализации угроз безопасности информации (Н3);

высокими возможностями по реализации угроз безопасности информации (Н4).

Для одной системы или сети актуальными могут являться нарушители, имеющие разные уровни возможностей.

Уровни возможностей нарушителей по реализации угроз безопасности информации приведены в приложении 8 к настоящей Методике.

5.1.6. Для актуальных нарушителей должны быть определены их категории в зависимости от имеющихся прав и условий по доступу к системам и сетям, обусловленных архитектурой и условиями функционирования этих систем и сетей, а также от установленных возможностей нарушителей. При этом нарушители подразделяются на две категории (рисунок 5, 6):

внешние нарушители – нарушители, не имеющие прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации;

внутренние нарушители – нарушители, имеющие права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей.

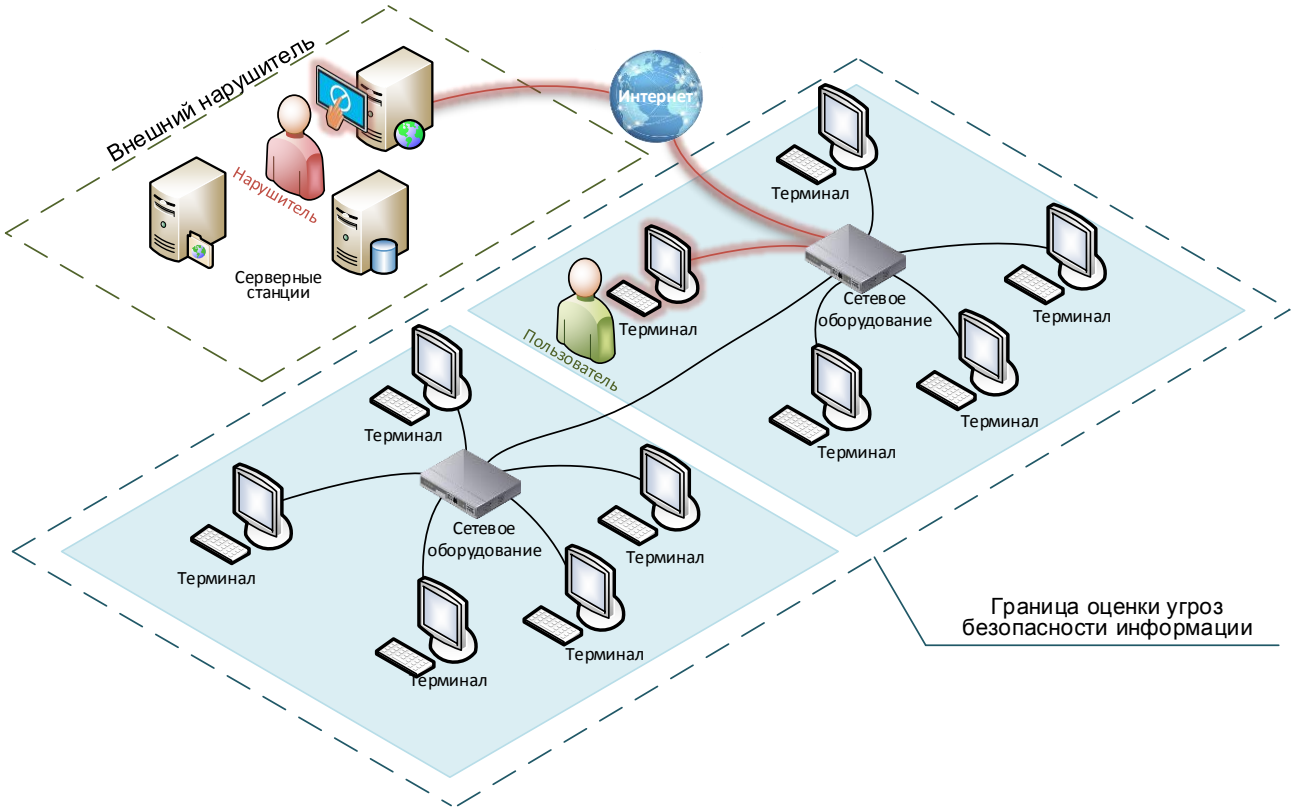

Рисунок 5. Внешний нарушитель при реализации угроз безопасности информации

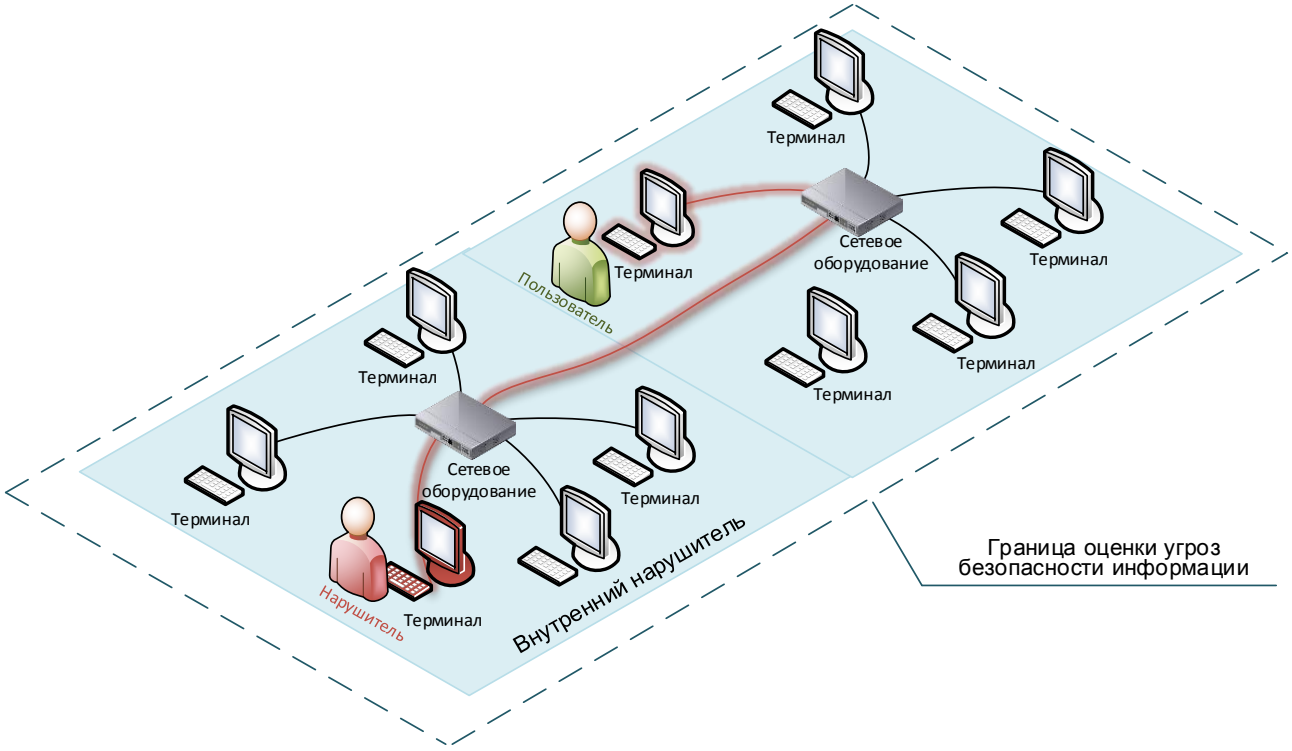

Рисунок 6. Внутренний нарушитель при реализации угроз безопасности информации

Внутренние нарушители первоначально могут иметь разный уровень прав доступа к информационным ресурсам и компонентам систем и сетей (например, доступ в личный кабинет на сайте, исполнение обязанностей на автоматизированном рабочем месте, администрирование систем и сетей). К внутренним нарушителям относятся пользователи, имеющие как непривилегированные (пользовательские), так и привилегированные (административные) права доступа к информационным ресурсам и компонентам систем и сетей.

5.1.7. Внешние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых. Внутренние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых или непреднамеренно (непреднамеренные угрозы безопасности информации) без использования программных, программно-аппаратных средств.

***Пример 4**: к непреднамеренным угрозам безопасности информации могут относиться:*
1) нарушение функционирования системы управления базы данных за счет ввода в поля данных информации, превышающей допустимый объем;
2) нарушение функционирования веб-ресурса за счет того, что системный администратор допустил ошибку при выборе конфигурационного файла веб-сервера.

5.1.8. В случае если к системам и сетям предъявлены требования к устойчивости и надежности функционирования (в части целостности и доступности информационных ресурсов и компонентов систем и сетей), дополнительно к антропогенным источникам угроз безопасности информации в качестве актуальных могут быть определены техногенные источники (физические явления, материальные объекты). Угрозы безопасности информации, связанные с техногенными источниками, включаются в модель угроз безопасности информации по решению обладателя информации или оператора систем и сетей.

Основными факторами возникновения угроз безопасности информации, связанными с техногенными источниками, могут являться:

а) недостатки качества, надежности программного обеспечения, программно-аппаратных средств, обеспечивающих обработку и хранение информации, их линий связи;

б) недостатки в работе обеспечивающих систем;

в) недоступность сервисов (услуг), предоставляемых сторонними организациями.

Возможность возникновения таких угроз определяется на основе статистики их возникновения за прошлые годы. В случае отсутствия указанной статистики возможно использование экспертной оценки.

Выявление техногенных источников должно осуществляться с учетом требований и правил, установленных уполномоченными федеральными органами исполнительной власти, национальными стандартами[1], и не входит в область действия данной Методики.

5.1.9. По результатам определения источников угроз безопасности информации должны быть определены:

а) виды актуальных нарушителей и возможные цели реализации ими угроз безопасности информации, а также их возможности;

б) категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы.

При определении источников угроз безопасности информации необходимо исходить из предположения о наличии повышенной мотивации

[1] Например, такими стандартами являются:
ГОСТ Р 22.0.05-2020 Безопасность в чрезвычайных ситуациях. Техногенные чрезвычайные ситуации. Термины и определения;
ГОСТ Р 51901.1-2002 Менеджмент риска. Анализ риска технологических систем (с Поправкой).

внешних и внутренних нарушителей, преднамеренно реализующих угрозы безопасности информации. Кроме того, необходимо учитывать, что такие виды нарушителей как специальные службы иностранных государств и террористические, экстремистские группировки могут привлекать (входить в сговор) внутренних нарушителей, в том числе обладающих привилегированными правами доступа. В этом случае уровень возможностей актуальных нарушителей будет определяться совокупностью возможностей нарушителей, входящих в сговор.

Примеры определения актуальных нарушителей при реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности приведены в приложении 9 к настоящей Методике.

5.2 Оценка способов реализации (возникновения) угроз безопасности информации

5.2.1. В ходе оценки угроз безопасности информации должны быть определены возможные способы реализации (возникновения) угроз безопасности информации, за счет использования которых актуальными нарушителями могут быть реализованы угрозы безопасности информации в системах и сетях, – актуальные способы реализации (возникновения) угроз безопасности информации.

5.2.2. Исходными данными для определения актуальных способов реализации (возникновения) 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. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

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

в) документация на системы и сети (в части сведений о составе и архитектуре, о группах пользователей и их типах доступа и уровней полномочий, о внешних и внутренних интерфейсах);

г) негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с настоящей Методикой;

д) объекты воздействия угроз безопасности информации и соответствующие им виды воздействия, определенные в соответствии с настоящей Методикой;

е) виды и категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы, и их возможности, определенные в соответствии с настоящей Методикой.

Указанные исходные данные могут быть дополнены иными документами и сведениями с учетом особенностей области деятельности, в которой функционируют системы и сети.

5.2.3. На основе анализа исходных данных, а также возможностей нарушителей определяются способы реализации (возникновения) угроз безопасности информации, актуальные для систем и сетей.

Основными способами реализации (возникновения) угроз безопасности информации являются:

1) использование уязвимостей (уязвимостей кода (программного обеспечения), уязвимостей архитектуры и конфигурации систем и сетей, а также организационных и многофакторных уязвимостей);

2) внедрение вредоносного программного обеспечения;

3) использование недекларированных возможностей программного обеспечения и (или) программно-аппаратных средств;

4) установка программных и (или) программно-аппаратных закладок в программное обеспечение и (или) программно-аппаратные средства;

5) формирование и использование скрытых каналов (по времени, по памяти) для передачи конфиденциальных данных;

6) перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей) для доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;

7) инвазивные способы доступа к конфиденциальной информации, содержащейся в аппаратных средствах аутентификации;

8) нарушение безопасности при поставках программных, программно-аппаратных средств и (или) услуг по установке, настройке, испытаниям, пусконаладочным работам (в том числе администрированию, обслуживанию);

9) ошибочные действия в ходе создания и эксплуатации систем и сетей, в том числе при установке, настройке программных и программно-аппаратных средств.

Указанные способы реализации (возникновения) угроз безопасности информации могут быть дополнены иными способами с учетом особенностей архитектуры и условий функционирования систем и сетей.

Способы реализации (возникновения) угроз безопасности информации определяются применительно к объектам воздействия, определенным в соответствии с настоящей Методикой. Способы являются актуальными, когда возможности нарушителя позволяют их использовать для реализации угроз безопасности и имеются или созданы условия, при которых такая возможность может быть реализована в отношении объектов воздействия. Одна угроза безопасности информации может быть реализована несколькими способами.

5.2.4. Условием, позволяющим нарушителям использовать способы реализации угроз безопасности информации, является наличие у них возможности доступа к следующим типам интерфейсов объектов воздействия:

внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями

(проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);

внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами систем и сетей, имеющими внешние сетевые интерфейсы (проводные, беспроводные);

интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);

интерфейсы для использования съемных машинных носителей информации и периферийного оборудования;

интерфейсы для установки, настройки, испытаний, пусконаладочных работ (в том числе администрирования, управления, обслуживания) обеспечения функционирования компонентов систем и сетей;

возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей.

Наличие указанных интерфейсов определяется архитектурой, составом и условиями функционирования систем и сетей, группами пользователей, их типами доступа и уровнями полномочий. В ходе анализа должны быть определены как логические, так и физические интерфейсы объектов воздействия, в том числе требующие физического доступа к ним.

Интерфейсы определяются на аппаратном, системном и прикладном уровнях систем и сетей, а также для телекоммуникационного оборудования. Возможность их использования на указанных уровнях определяется возможностями актуальных нарушителей.

5.2.5. На этапе создания систем и сетей определение интерфейсов объектов воздействия, которые могут использоваться для реализации угроз безопасности, проводится на основе предполагаемой архитектуры и условий функционирования систем и сетей, определенных на основе изучения и анализа исходных данных о них.

На этапе эксплуатации систем и сетей для определения интерфейсов объектов воздействия, которые могут использоваться для реализации угроз безопасности, дополнительно к документации на сети и системы используются результаты инвентаризации систем и сетей, проведенной с использованием автоматизированных средств.

5.2.6. По результатам оценки возможных способов реализации угроз безопасности информации должны быть определены:

а) виды и категории нарушителей, которые имеют возможность использования актуальных способов;

б) актуальные способы реализации угроз безопасности информации и типы интерфейсов объектов воздействия, за счет которых они могут быть реализованы.

Примеры определения актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности приведены в приложении 10 к настоящей Методике.

5.3 Оценка актуальности угроз безопасности информации

5.3.1. В ходе оценки угроз безопасности информации должны быть определены возможные угрозы безопасности информации и оценена их актуальность для систем и сетей – актуальные угрозы безопасности информации.

5.3.2. Исходными данными для оценки актуальности 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. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

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

в) негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с настоящей Методикой;

г) объекты воздействия угроз безопасности информации и виды воздействий на них, определенные в соответствии с настоящей Методикой;

д) виды и категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы, и их возможности, определенные в соответствии с настоящей Методикой;

е) актуальные способы реализации (возникновения) угроз безопасности информации.

5.3.3. На основе анализа исходных данных определяются возможные для систем и сетей угрозы безопасности информации, к которым относятся осуществляемые нарушителем воздействия на информационные ресурсы и компоненты систем и сетей (объекты воздействия), в результате которых возможно нарушение безопасности информации и (или) нарушение или прекращение функционирования систем и сетей.

Угроза безопасности информации возможна, если имеются нарушитель или иной источник угрозы, объект, на который осуществляются воздействия, способы реализации угрозы безопасности информации, а реализация угрозы может привести к негативным последствиям:

$УБИ_i$ = [нарушитель (источник угрозы); объекты воздействия; способы реализации угроз; негативные последствия].

5.3.4. Актуальность возможных угроз безопасности информации определяется наличием сценариев их реализации.

Сценарии реализации угроз безопасности информации должны быть определены для соответствующих способов реализации угроз безопасности информации, определенных в соответствии с настоящей Методикой, и применительно к объектам воздействия и видам воздействия на них. Определение сценариев предусматривает установление последовательности возможных тактик и соответствующих им техник, применение которых возможно актуальным нарушителем с соответствующим уровнем возможностей, а также доступности интерфейсов для использования соответствующих способов реализации угроз безопасности информации.

Перечень основных тактик (тактических задач) и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации, приведен в приложении 11 к настоящей Методике.

5.3.5. На этапе создания систем и сетей должен быть определен хотя бы один сценарий каждого способа реализации возможной угрозы безопасности информации. Сценарий определяется для каждого актуального нарушителя и их уровней возможностей.

При наличии хотя бы одного сценария угрозы безопасности информации такая угроза признается актуальной для системы и сети и включается в модель угроз безопасности систем и сетей для обоснования выбора организационных и технических мер по защите информации (обеспечению безопасности), а также выбора средств защиты информации (рисунок 7).

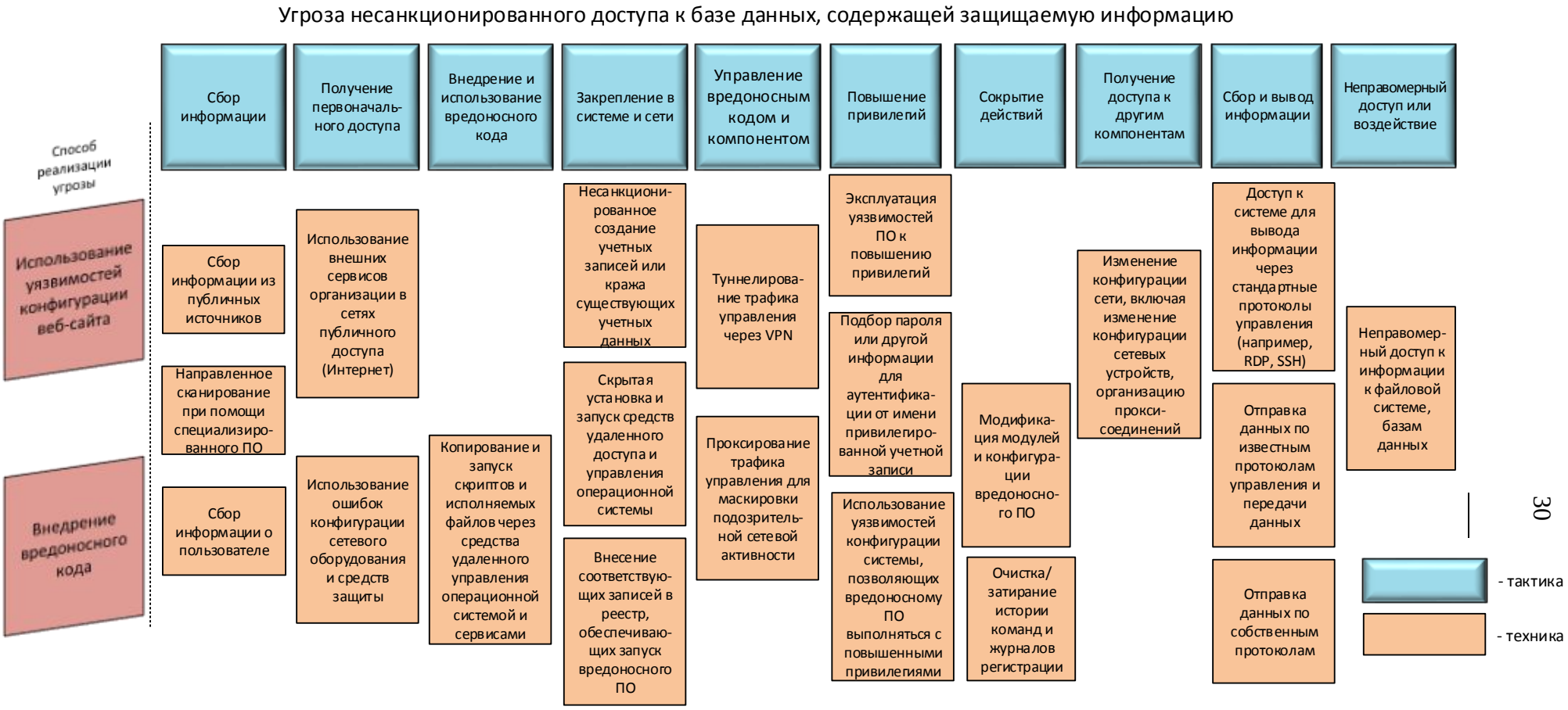

Рисунок 7. Пример сценария реализации угрозы безопасности информации

На этапе эксплуатации систем и сетей для каждой возможной угрозы безопасности информации определяется множество возможных сценариев ее реализации в интересах оценки эффективности принятых технических мер по защите информации (обеспечению безопасности), в том числе средств защиты информации. При этом множество сценариев определяется для каждого актуального нарушителя и уровней его возможностей в соответствии с полученными результатами инвентаризации систем и сетей, анализа уязвимостей и (или) тестирования на проникновение, проведенных с использованием автоматизированных средств (рисунок 8).

5.3.6. На этапе эксплуатации определение сценариев реализации угрозы включает:

а) анализ исходных данных на систему или сеть, предусматривающий в том числе анализ документации, модели угроз безопасности информации, применяемых средств защиты информации, и определение планируемых к применению автоматизированных средств;

б) проведение инвентаризации информационных систем и сетей и определение объектов воздействия и их интерфейсов;

в) определение внешних интерфейсов, которые могут быть задействованы при реализации угроз безопасности информации;

г) определение внутренних интерфейсов, которые могут быть задействованы при реализации угроз безопасности информации;

д) выявление уязвимостей объектов воздействия, а также компонентов систем и сетей, имеющих внешние интерфейсы, с которыми посредством внутренних интерфейсов взаимодействуют объекты воздействия;

е) проведение тестирования на проникновение, подтверждающего возможность использования выявленных уязвимостей или выявления новых сценариев реализации угрозы безопасности информации;

ж) поиск последовательности тактик и техник, применение которых может привести к реализации угрозы безопасности информации, исходя из уровня возможностей актуальных нарушителей, а также результатов инвентаризации, анализа уязвимостей и тестирования на проникновение;

з) составление сценариев реализации угрозы безопасности информации применительно к объектам и видам воздействия, а также способам реализации угроз безопасности информации.

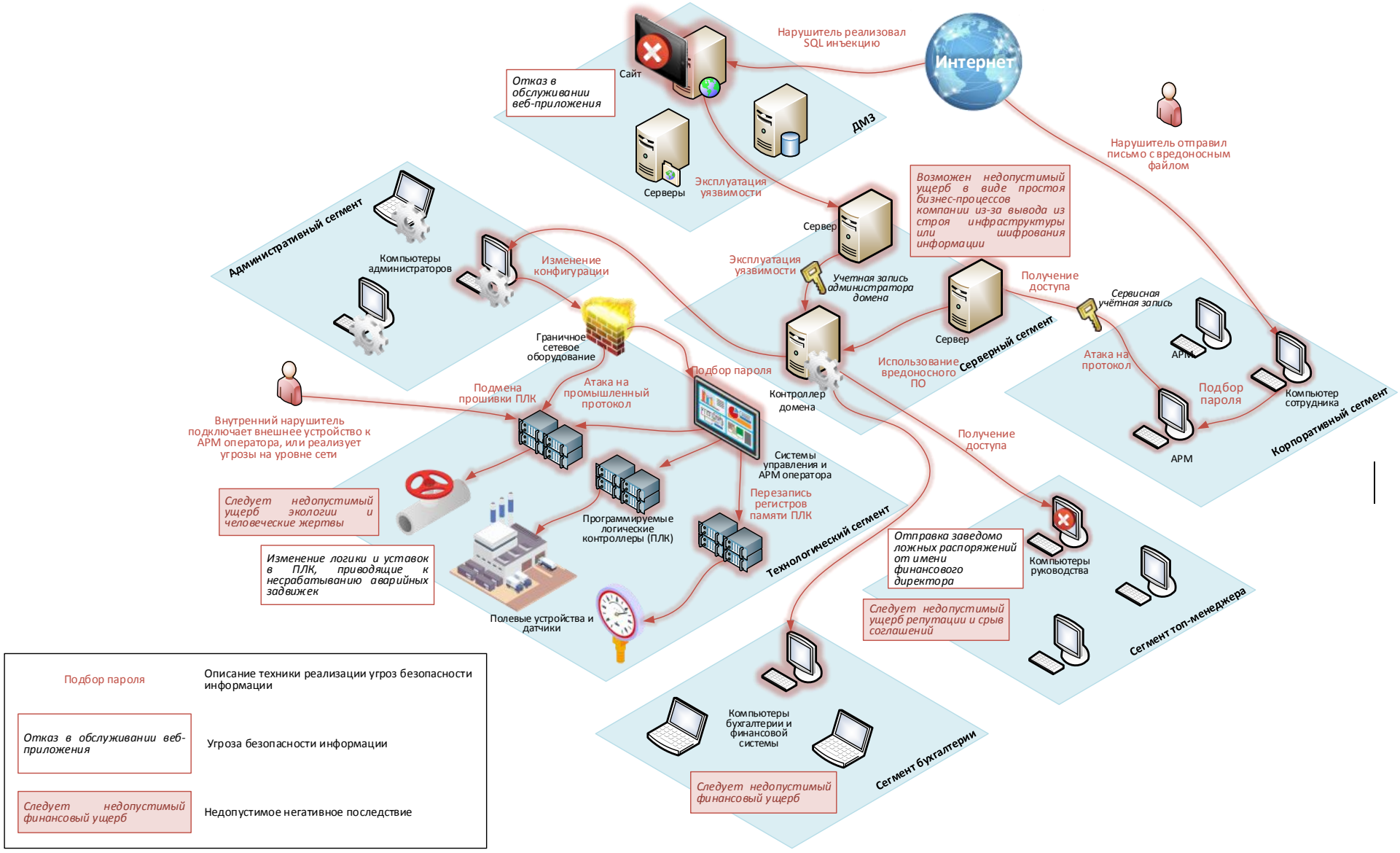

Рисунок 8. Пример сценариев реализации угроз безопасности информации

Приложение 1
к Методике оценки угроз
безопасности информации

Термины и определения, применяемые для целей настоящего методического документа

Архитектура систем и сетей: совокупность основных структурно-функциональных характеристик, свойств, компонентов систем и сетей, воплощенных в информационных ресурсах и компонентах, правилах их взаимодействия, режимах обработки информации.

Взаимодействующая (смежная) система: система или сеть, которая в рамках установленных функций имеет взаимодействие посредством сетевых интерфейсов с системой и сетью оператора и не включена им в границу процесса оценки угроз безопасности информации.

Возможности нарушителя: мера усилий нарушителя для реализации угрозы безопасности информации, выраженная в показателях компетентности, оснащенности ресурсами и мотивации нарушителя.

Граница оценки угроз безопасности информации: совокупность информационных ресурсов и компонентов систем и сетей, в пределах которой обеспечивается защита информации (безопасность) в соответствии с едиными правилами и процедурами, а также контроль за реализованными мерами защиты информации (обеспечения безопасности).

Информационные ресурсы: информация, данные, представленные в форме, предназначенной для хранения и обработки в системах и сетях.

Компонент (системы, сети): программное, программно-аппаратное или техническое средство, входящее в состав систем и сетей.

Обеспечивающие системы: инженерные системы, включающие системы электроснабжения, вентиляции, охлаждения, кондиционирования, охраны и другие инженерные системы, а также средства, каналы и системы, предназначенные для оказания услуг связи, других услуг и сервисов, предоставляемых сторонними организациями, от которых зависит функционирование систем и сетей.

Обладатель информации: лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Оператор: лицо, осуществляющее деятельность по эксплуатации систем и сетей, в том числе по обработке содержащейся в них информации**.**

Основные (критические) процессы (бизнес-процессы): управленческие, организационные, технологические, производственные, финансово-экономические и иные основные процессы (бизнес-процессы), выполняемые обладателем информации, оператором в рамках реализации функций (полномочий) или осуществления основных видов деятельности,

нарушение и (или) прекращение которых может привести к возникновению рисков (ущербу).

Пользователь: лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в системе или сети и использующее результаты ее функционирования.

Поставщик услуг: лицо, предоставляющее оператору и (или) обладателю на основании договора или ином законном основании услуги по использованию своих вычислительных ресурсов, программного обеспечения, средств хранения или передачи информации.

Программно-аппаратное средство: устройство, состоящее из аппаратного обеспечения и функционирующего на нем программного обеспечения, участвующее в формировании, обработке, передаче или приеме информации.

Угроза безопасности информации: совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Уязвимость: недостаток (слабость) программного (программно-технического) средства или системы и сети в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации.

Приложение 2
к Методике оценки угроз
безопасности информации

Рекомендации по формированию экспертной группы и проведению экспертной оценки при оценке 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 мене 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		

Приложение 3
к Методике оценки угроз
безопасности информации

Рекомендуемая структура модели 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.

Приложение 4
к Методике оценки угроз
безопасности информации

Виды рисков (ущерба) и типовые негативные последствия от реализации угроз безопасности информации

Таблица 4.1

№	Виды риска (ущерба)	Возможные типовые негативные последствия
У1	Ущерб физическому лицу	Угроза жизни или здоровью. Унижение достоинства личности. Нарушение свободы, личной неприкосновенности. Нарушение неприкосновенности частной жизни. Нарушение личной, семейной тайны, утрата чести и доброго имени. Нарушение тайны переписки, телефонных переговоров, иных сообщений. Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах. Финансовый, иной материальный ущерб физическому лицу. Нарушение конфиденциальности (утечка) персональных данных. «Травля» гражданина в сети «Интернет». Разглашение персональных данных граждан
У2	Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью	Нарушение законодательства Российской Федерации. Потеря (хищение) денежных 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). Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. Срыв запланированной сделки с партнером. Необходимость дополнительных (незапланированных) затрат на восстановление деятельности.

Продолжение таблицы 4.1

№	Виды риска (ущерба)	Возможные типовые негативные последствия
		Потеря клиентов, поставщиков. Потеря конкурентного преимущества. Невозможность заключения договоров, соглашений. Нарушение деловой репутации. Снижение престижа. Дискредитация работников. Утрата доверия. Причинение имущественного ущерба. Неспособность выполнения договорных обязательств. 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 сети. Публикация недостоверной информации на веб-ресурсах организации. Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением. Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени. Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)
У3	Ущерб государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	Причинение ущерба жизни и здоровью людей. Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения. Прекращение или нарушение функционирования объектов транспортной инфраструктуры. Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия). Прекращение или нарушение функционирования сети связи. Отсутствие доступа к государственной услуге. Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации. Снижение уровня дохода государственной корпорации, государственной организации или организации с государственным участием.

Продолжение таблицы 4.1

№	Виды риска (ущерба)	Возможные типовые негативные последствия
		Возникновение ущерба бюджетам Российской Федерации. Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций в системно значимой кредитной организации, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем, системно значимой инфраструктурной организацией финансового рынка. Вредные воздействия на окружающую среду. Прекращение или нарушение функционирования пункта управления (ситуационного центра). Снижение показателей государственного оборонного заказа. Прекращение или нарушение функционирования информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка. Нарушение законодательства Российской Федерации. Публикация недостоверной социально значимой информации на веб-ресурсах, которая может привести к социальной напряженности, панике среди населения и др. Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса, если это ведет к выводу из строя технологических объектов, их компонентов. Нарушение общественного правопорядка, возможность потери или снижения уровня контроля за общественным правопорядком. Нарушение выборного процесса. Отсутствие возможности оперативного оповещения населения о чрезвычайной ситуации. Организация пикетов, забастовок, митингов и других акций. Массовые увольнения. Увеличение количества жалоб в органы государственной власти или органы местного самоуправления. Появление негативных публикаций в общедоступных источниках. Создание предпосылок к внутриполитическому кризису.

Окончание таблицы 4.1

№	Виды риска (ущерба)	Возможные типовые негативные последствия
		Доступ к персональным данным сотрудников органов государственной власти, уполномоченных в области обеспечения обороны, безопасности и правопорядка, высших должностных лиц государственных органов и других лиц государственных органов. Доступ к системам и сетям с целью незаконного использования вычислительных мощностей. Использование веб-ресурсов государственных органов для распространения и управления вредоносным программным обеспечением. Утечка информации ограниченного доступа. Непредоставление государственных услуг

Указанные типовые негативные последствия от реализации угроз безопасности информации подлежат конкретизации и могут дополняться другими негативными последствиями в зависимости от особенностей области деятельности, в которой функционирует система и сеть.

Приложение 5
к Методике оценки угроз
безопасности информации

Примеры определения объектов воздействия и видов воздействия на них

Таблица 5.1

Негативные последствия	Объекты воздействия	Виды воздействия
Разглашение персональных данных граждан (У1)	База данных информационной системы, содержащая идентификационную информацию граждан	Утечка идентификационной информации граждан из базы данных
	Удаленное автоматизированное рабочее место (АРМ) пользователя	Утечка идентификационной информации граждан с АРМ пользователя
	Линия связи между сервером основного центра обработки данных и сервером резервного центра обработки данных	Перехват информации, содержащей идентификационную информацию граждан, передаваемой по линиям связи
	Веб-приложение информационной системы, обрабатывающей идентификационную информацию граждан	Несанкционированный доступ к идентификационной информации граждан, содержащейся в веб-приложении информационной системы
Хищение денежных средств со счета организации (У2)	Банк-клиент	Несанкционированная подмена данных, содержащихся в реквизитах платежного поручения
	АРМ финансового директора	Несанкционированная модификация информации в платежных распоряжениях и отправка недостоверных распоряжений от имени финансового директора
	Электронный почтовый ящик финансового директора	Модификация информации в платежных распоряжениях и отправка недостоверных распоряжений от имени финансового директора
	АРМ главного бухгалтера	Подмена данных, содержащих реквизиты платежных поручений и другой платежной информации на АРМ главного бухгалтера

Окончание таблицы 5.1

Негативные последствия	Объекты воздействия	Виды воздействия
Срыв запланированной сделки с партнером (У2)	АРМ руководителя организации	Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя организации
	Электронный почтовый ящик руководителя организации	Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя организации
Загрязнения окружающей среды и водоемов в результате разлива нефти из нефтепровода (У3)	Коммутационный контроллер для управления аварийными задвижками в нефтепроводе	Несанкционированная модификация (изменение) логики работы или уставок коммутационного контроллера, которая приводит к открытию (или не закрытию) аварийной задвижки при нарушении герметичности нефтепровода
	Программируемый логический контроллер (ПЛК) для управления насосными станциями	Несанкционированная модификация (изменение) логики работы или уставок ПЛК, которая приводит к включению (или не отключению) насосной станции при закрытой аварийной задвижке в нефтепроводе
	АРМ оператора	Несанкционированная отправка команд, приводящая к несрабатыванию средств аварийной защиты и (или) к изменению логики ПЛК
Непредоставление государственных услуг (У3)	Веб-приложение портала государственных услуг	Отказ в обслуживании веб-приложения
	Система управления содержимым веб-приложения (сайта) портала государственных услуг	Подмена информации на страницах портала на недостоверную
	Сервер балансировки нагрузки на веб-приложение (сайт) портала государственных услуг	Отказ в обслуживании веб-приложения
	Сервер веб-приложения (сайта) портала государственных услуг	Отказ в обслуживании веб-приложения
	Сервер баз данных портала государственных услуг	Отказ в обслуживании сервера управления базами данных
		Подмена информации в базах данных на недостоверную
		Утечка персональных данных граждан

Приложение 6
к Методике оценки угроз
безопасности информации

Возможные цели реализации угроз безопасности информации нарушителями

Таблица 6.1

№ вида	Виды нарушителя	Категории нарушителя	Возможные цели реализации угроз безопасности информации
1	Специальные службы иностранных государств	Внешний	Нанесение ущерба государству в области обеспечения обороны, безопасности и правопорядка, а также в иных отдельных областях его деятельности или секторах экономики, в том числе дискредитация или дестабилизация деятельности отдельных органов государственной власти, организаций, получение конкурентных преимуществ на уровне государства, срыв заключения международных договоров, создание внутриполитического кризиса
2	Террористические, экстремистские группировки	Внешний	Совершение террористических актов, угроза жизни граждан. Нанесение ущерба отдельным сферам деятельности или секторам экономики государства. Дестабилизация общества. Дестабилизация деятельности органов государственной власти, организаций
3	Преступные группы (криминальные структуры)	Внешний	Получение финансовой или иной материальной выгоды. Желание самореализации (подтверждение статуса)
4	Отдельные физические лица (хакеры)	Внешний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса)
5	Конкурирующие организации	Внешний	Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды
6	Разработчики программных, программно-аппаратных средств	Внутренний	Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки. Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия

Окончание таблицы 6.1

№ вида	Виды нарушителя	Категории нарушителя	Возможные цели реализации угроз безопасности информации
7	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ
8	Поставщики вычислительных услуг, услуг связи	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ
9	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ
10	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия
11	Авторизованные пользователи систем и сетей	Внутренний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
12	Системные администраторы и администраторы безопасности	Внутренний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
13	Бывшие работники (пользователи)	Внешний	Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия

Указанные возможные цели реализации угроз безопасности информации подлежат конкретизации и могут дополняться другими целями в зависимости от особенностей области деятельности, в которой функционируют системы и сети.

При оценке возможностей нарушителей необходимо исходить из того, что для повышения уровня своих возможностей нарушители 1 вида могут вступать

в сговор с нарушителями 5, 6, 7, 8, 9, 10, 11, 12 видов. Нарушители 2 вида могут вступать в сговор с нарушителями 10, 11, 12 видов. Нарушители 3 вида могут вступать в сговор с нарушителями 10, 11, 12 видов. В случае принятия таких предположений цели и уровни возможностей нарушителей подлежат объединению.

Приложение 7
к Методике оценки угроз
безопасности информации

Пример оценки целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации (для государственной информационной системы)

Таблица 7.1

Виды нарушителей	**Возможные цели реализации угроз безопасности информации**			**Соответствие целей видам риска (ущерба) и возможным негативным последствиям**
	Нанесение ущерба физическому лицу	**Нанесение ущерба юридическому лицу, индивидуальному предпринимателю**	**Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности**	
Специальные службы иностранных государств	-	-	+ (дискредитация или дестабилизация деятельности органа государственной власти*)	У3** (нарушение функционирования государственного органа, дискредитация деятельности органа государственной власти)
Террористические, экстремистские группировки	-	-	+ (дестабилизация деятельности органов государственной власти, организаций)	У3 (отсутствие доступа к социально значимым государственным услугам)

Продолжение таблицы 7.1

Виды нарушителей	**Возможные цели реализации угроз безопасности информации**			**Соответствие целей видам риска (ущерба) и возможным негативным последствиям**
	Нанесение ущерба физическому лицу	**Нанесение ущерба юридическому лицу, индивидуальному предпринимателю**	**Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности**	
Преступные группы (криминальные структуры)	+ (получение финансовой выгоды за счет кражи и продажи персональных данных граждан)	+ (получение финансовой выгоды за счет использования вычислительных мощностей серверов государственной информационной системы для майнинга криптовалюты)	+ (желание самореализоваться)	У1 (нарушение конфиденциальности персональных данных граждан) У2 (нарушение деловой репутации) У3 (организация митингов, забастовок из-за публикаций недостоверной информации)
Отдельные физические лица (хакеры)	+ (желание самореализоваться)	+ (получение финансовой выгоды за счет кражи и коммерческой тайны)	-	У1 (нарушение личной, семейной тайны, утрата чести и доброго имени) У2 (утечка коммерческой тайны; потеря клиентов)
Конкурирующие организации	-	-	-	-

Продолжение таблицы 7.1

Виды нарушителей	**Возможные цели реализации угроз безопасности информации**			**Соответствие целей видам риска (ущерба) и возможным негативным последствиям**
	Нанесение ущерба физическому лицу	**Нанесение ущерба юридическому лицу, индивидуальному предпринимателю**	**Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности**	
Разработчики программных, программно-аппаратных средств	-	+ (передача информации о юридическом лице третьим лицам)	+ (внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки при вступлении в сговор со специальными службами иностранных государств)	У2 (недополучение ожидаемой прибыли) У3 (нарушение функционирования государственного органа, дискредитация деятельности органа государственной власти)
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	-	-	-	-
Поставщики вычислительных услуг, услуг связи	-	-	-	-
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	-	-	-	-

Продолжение таблицы 7.1

Виды нарушителей	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	
Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	-	-	-	-
Авторизованные пользователи систем и сетей	+ (непреднамеренные, неосторожные или неквалифицированные действия)	-	-	У1 (финансовый, иной материальный ущерб физическим лицам)
Системные администраторы и администраторы безопасности	+ (месть за ранее совершенные действия)	+ (любопытство или желание самореализации)	+ (получение финансовой или иной материальной выгоды при вступлении в сговор с преступной группой)	У1 (финансовый, иной материальный ущерб физическим лицам) У2 (невозможность заключения договоров, соглашений) У3 (утечка информации ограниченного доступа)

Окончание таблицы 7.1

Виды нарушителей	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	
Бывшие (уволенные) работники (пользователи)	-	-	-	-

[*] - примеры возможных целей реализации угроз безопасности информации с учетом области деятельности, в которой функционируют системы и сети, определенные в соответствии с приложением 6 к настоящей Методике.

[**]- примеры сопоставления возможных целей реализации угроз безопасности информации с видами ущерба (риска) и возможными негативными последствиями о реализации угроз, определенные в соответствии с приложением 5 к настоящей Методике.

Приложение 8
к Методике оценки угроз
безопасности информации

Уровни возможностей нарушителей по реализации угроз безопасности информации

Таблица 8.1

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
Н1	Нарушитель, обладающий базовыми возможностями	Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. Обладает базовыми компьютерными знаниями и навыками на уровне пользователя. Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним. **Таким образом, нарушители с базовыми возможностями имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов**	Физическое лицо (хакер) Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем (администрация, охрана, уборщики и т.д.) Авторизованные пользователи систем и сетей Бывшие работники (пользователи)
Н2	Нарушитель, обладающий базовыми повышенными возможностями	Обладает всеми возможностями нарушителей с базовыми возможностями. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, однако хорошо владеет этими	Преступные группы (два лица и более, действующие по единому плану) Конкурирующие организации Поставщики вычислительных услуг,

Продолжение таблицы 8.1

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
		средствами и инструментами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз. Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации. Обладает практическими знаниями о функционировании систем и сетей, операционных систем, а также имеет знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. **Таким образом, нарушители с базовыми повышенными возможностями имеют возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей**	услуг связи Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ Системные администраторы и администраторы безопасности
Н3	Нарушитель, обладающий средними возможностями	Обладает всеми возможностями нарушителей с базовыми повышенными возможностями. Имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность приобретать дорогостоящие средства и инструменты для реализации угроз, размещаемые на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность самостоятельно разрабатывать средства	Террористические, экстремистские группировки Разработчики программных, программно-аппаратных средств

Продолжение таблицы 8.1

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
		(инструменты), необходимые для реализации угроз (атак), реализовывать угрозы с использованием данных средств. Имеет возможность получения доступа к встраиваемому программному обеспечению аппаратных платформ, системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-аппаратным средствам для проведения их анализа. Обладает знаниями и практическими навыками проведения анализа программного кода для получения информации об уязвимостях. Обладает высокими знаниями и практическими навыками о функционировании систем и сетей, операционных систем, а также имеет глубокое понимание защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. Имеет возможность реализовывать угрозы безопасности информации в составе группы лиц. **Таким образом, нарушители со средними возможностями имеют возможность реализовывать угрозы, в том числе на выявленные ими неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей**	
Н4	Нарушитель, обладающий высокими возможностями	Обладает всеми возможностями нарушителей со средними возможностями. Имеет возможность получения доступа к исходному коду встраиваемого программного обеспечения аппаратных платформ, системного и прикладного программного обеспечения, телекоммуникационного оборудования и других программно-аппаратных средств для получения сведений об уязвимостях «нулевого дня». Имеет возможность внедрения программных (программно-аппаратных) закладок или уязвимостей на различных этапах поставки программного обеспечения или программно-аппаратных средств.	Специальные службы иностранных государств

Окончание таблицы 8.1

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
		Имеет возможность создания методов и средств реализации угроз с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение. Имеет возможность реализовывать угрозы с привлечением специалистов, имеющих базовые повышенные, средние и высокие возможности. Имеет возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений. Имеет возможность долговременно и незаметно для операторов систем и сетей реализовывать угрозы безопасности информации. Обладает исключительными знаниями и практическими навыками о функционировании систем и сетей, операционных систем, аппаратном обеспечении, а также осведомлен о конкретных защитных механизмах, применяемых в программном обеспечении, программно-аппаратных средствах атакуемых систем и сетей. **Таким образом, нарушители с высокими возможностями имеют практически неограниченные возможности реализовывать угрозы, в том числе с использованием недекларированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей**	

Приложение 9
к Методике оценки угроз
безопасности информации

Примеры результата определения актуальных нарушителей при реализации угроз безопасности информации и соответствующие им возможности (для государственной информационной системы)

Таблица 9.1

№ п/п	Виды риска (ущерба) и возможные негативные последствия*	Виды актуального нарушителя**	Категория нарушителя	Уровень возможностей нарушителя
1	У1: нарушение конфиденциальности персональных данных граждан; нарушение личной, семейной тайны, утрата чести и доброго имени; финансовый, иной материальный ущерб физических лиц	Преступные группы (криминальные структуры)	Внешний Внутренний***	Н3
		Отдельные физические лица (хакеры)	Внешний	Н2
		Разработчики программных, программно-аппаратных средств	Внутренний	Н3
		Системные администраторы и администраторы безопасности	Внутренний	Н2
		Авторизованные пользователи систем и сетей	Внутренний	Н2
2	У2: невозможность заключения договоров, соглашений; утечка коммерческой тайны; потеря клиентов; нарушение деловой репутации; недополучение ожидаемой прибыли	Преступные группы (криминальные структуры)	Внешний	Н3
		Отдельные физические лица (хакеры)	Внутренний	Н2
		Разработчики программных, программно-аппаратных средств	Внутренний	Н3
		Системные администраторы и администраторы безопасности	Внутренний	Н2
3	У3: нарушение функционирования государственного органа, дискредитация деятельности органа	Специальные службы иностранных государств	Внешний Внутренний***	Н4
		Террористические, экстремистские организации	Внешний	Н3

Окончание таблицы 9.1

№ п/п	Виды риска (ущерба) и возможные негативные последствия*	Виды актуального нарушителя**	Категория нарушителя	Уровень возможностей нарушителя
	государственной власти; доступ к системам и сетям с целью незаконного использования вычислительных мощностей; утечка информации ограниченного доступа; организация митингов, забастовок из-за публикаций недостоверной информации; отсутствие доступа к социально значимым государственным услугам	Преступные группы (криминальные структуры)	Внешний Внутренний***	Н3
		Разработчики программных, программно-аппаратных средств	Внутренний	Н3
		Системные администраторы и администраторы безопасности	Внутренний	Н3
		Авторизованные пользователи систем и сетей	Внутренний	Н1
		Бывшие (уволенные) работники (пользователи)	Внутренний	Н1

* - примеры возможных целей реализации угроз безопасности информации с учетом области деятельности, в которой функционируют системы и сети, определенные с учетом приложений 4 и 5 к настоящей Методике.

** - примеры видов актуальных нарушителей, определенные с учетом приложений 6 и 7 к настоящей Методике.

*** - при сговоре преступной группировки (криминальной структуры) с системными администраторами и администраторами безопасности, определенном в приложении 7 к настоящей Методике.

Приложение 10
к Методике оценки угроз
безопасности информации

Примеры определения актуальных способов реализации угроз безопасности информации и соответствующие им виды нарушителей и их возможности (для государственной информационной системы)

Таблица 10.1

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
1	Специальные службы иностранных государств (Н4)	Внешний	База данных информационной системы, содержащая идентификационную информацию граждан: несанкционированный доступ к компонентам систем или сетей, защищаемой информации, системным, конфигурационным, иным служебным данным; утечка (нарушение конфиденциальности) защищаемой информации, системных, конфигурационных, иных служебных данных	Веб-интерфейс удаленного администрирования базы данных информационной системы	Использование недекларированных возможностей программного обеспечения телекоммуникационного оборудования
				Пользовательский веб-интерфейс доступа к базе данных информационной системы	Использование уязвимостей конфигурации системы управления базами данных
			Линия связи между сервером основного центра обработки данных и сервером резервного центра обработки данных: перехват (нарушение конфиденциальности) защищаемой информации,	Канал передачи данных между сервером основного центра обработки данных и сервером резервного центра обработки данных	Установка программных закладок в телекоммуникационное оборудование

Продолжение таблицы 10.1

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
			системных, конфигурационных, иных служебных данных		
			Коммутационный контроллер для управления аварийными задвижками в нефтепроводе: нарушение функционирования (работоспособности) средств обработки и хранения информации; модификация (подмена) защищаемой информации, системных, конфигурационных, иных служебных данных	Удаленный канал управления коммутационным контроллером	Использование уязвимостей кода коммутационного контроллера
				Съемные машинные носители информации, содержащие аутентификационную информацию	Извлечение аутентификационной информации из постоянной памяти носителя (инвазивный метод)
2	Отдельные физические лица (хакеры) (Н2)	Внешний	Удаленное автоматизированное рабочее место (АРМ) пользователя: несанкционированный доступ к операционной системе АРМ пользователя; нарушение конфиденциальности информации, содержащейся на АРМ пользователя	Доступ через локальную вычислительную сеть организации	Внедрение вредоносного программного обеспечения
				Съемные машинные носители информации, подключаемые к АРМ пользователя	Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя
			Веб-сайт портала государственных услуг (сервисов): отказ в обслуживании веб-сайта портала государственных услуг	Веб-интерфейс пользователя веб-сайта государственных услуг	Использование уязвимостей кода программного обеспечения веб-сервера

Окончание таблицы 10.1

№ п/п	Вид нарушителя	Категория нарушителя	Объект воздействия	Доступные интерфейсы	Способы реализации
					Внедрение вредоносного кода в веб-приложение
				Сетевые интерфейсы коммутатора сети, где расположен веб-сервер	Использование уязвимостей конфигурации системы управления доступом к АРМ пользователя
3	Авторизованные пользователи систем и сетей (H1)	Внутренний	АРМ главного бухгалтера организации: модификация платежных поручений, хранящихся на АРМ главного бухгалтера	Локальная вычислительная сеть организации	Ошибочные действия в ходе настройки АРМ главного бухгалтера
			Сервер базы данных веб-сайта портала государственных услуг (сервисов): отказ в обслуживании отдельных компонентов или систем и сетей в целом	Веб-интерфейс системы администрирования веб-сайта портала государственных услуг	Нарушение цепочки услуг по администрированию портала государственных услуг

Приложение 11
к Методике оценки угроз
безопасности информации

Перечень основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации

Таблица 11.1

№	Тактика	Основные техники
Т1	Сбор информации о системах и сетях Тактическая задача: нарушитель стремится получить любую техническую информацию, которая может оказаться полезной в ходе реализации угроз безопасности информации	Т1.1. Сбор информации из публичных источников: официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций
		Т1.2. Сбор информации о подключенных к публичным системам и сетям устройствах и их службах при помощи поисковых систем, включая сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений. Пример: использование поисковой системы Shodan для получения информации об определенных моделях IP-камер видеонаблюдения с возможно уязвимыми версиями прошивок
		Т1.3. Пассивный сбор (прослушивание) информации о подключенных к сети устройствах с целью идентификации сетевых служб, типов и версий ПО этих служб и в некоторых случаях – идентификационной информации пользователей
		Т1.4. Направленное сканирование при помощи специализированного программного обеспечения подключенных к сети устройств с целью идентификации сетевых сервисов, типов и версий программного обеспечения этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений. Пример: сканирование при помощи сканера nmap
		Т1.5. Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, программного обеспечения сервисов и приложений путем поиска и эксплуатации уязвимостей подключенных к сети устройств. Пример: эксплуатация уязвимости типа directory traversal публично доступного веб-сервера

Продолжение таблицы 11.1

№	Тактика	Основные техники
		T1.6. Сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисами вычислительной сети, путем перебора. Пример: сбор информации о почтовых адресах при помощи directoryharvestattack на почтовые сервера
		T1.7. Сбор информации, предоставляемой DNS сервисами, включая DNS Hijacking
		T1.8. Сбор информации о пользователе при посещении им веб-сайта, в том числе с использованием уязвимостей программы браузера и надстраиваемых модулей браузера
		T1.9. Сбор информации о пользователях, устройствах, приложениях путем поиска информации в памяти, файлах, каталогах, базах данных, прошивках устройств, репозиториях исходных кодов ПО, включая поиск паролей в исходном и хэшированном виде, криптографических ключей. Пример: получение хэшей паролей из /etc/passwd или получение паролей по умолчанию путем обратного инжиниринга прошивки устройства
		T1.10. Кража цифровых сертификатов, включая кражу физических токенов, либо неавторизованное выписывание новых сертификатов (возможно после компрометации инфраструктуры доменного регистратора или аккаунта администратора зоны на стороне жертвы)
		T1.11. Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей путем применения социальной инженерии, в том числе фишинга
		T1.12. Сбор личной идентификационной информации (идентификаторы пользователей, устройств, информация об идентификации пользователей сервисами, приложениями, средствами удаленного доступа), в том числе сбор украденных личных данных сотрудников и подрядчиков на случай, если сотрудники/подрядчики используют одни и те же пароли на работе и за ее пределами
		T1.13. Сбор информации через получение доступа к системам физической безопасности и видеонаблюдения
		T1.14. Сбор информации через получение контроля над личными устройствами сотрудников (смартфонами, планшетами, ноутбуками) для скрытой прослушки и видеофиксации
		T1.15. Поиск и покупка баз данных идентификационной информации, скомпрометированых паролей и ключей на специализированных нелегальных площадках

Продолжение таблицы 11.1

№	Тактика	Основные техники
		T1.16. Сбор информации через получение доступа к базам данных результатов проведенных инвентаризаций, реестрам установленного оборудования и ПО, данным проведенных аудитов безопасности, в том числе через получение доступа к таким данным через компрометацию подрядчиков и партнеров
		T1.17. Пассивный сбор и анализ данных телеметрии для получения информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
		T1.18. Сбор и анализ данных о прошивках устройств, количестве и подключении этих устройств, используемых промышленных протоколах для получения информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
		T1.19. Сбор и анализ специфических для отрасли или типа предприятия характеристик технологического процесса для получения информации о технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
		T1.20. Техники конкурентной разведки и промышленного шпионажа для сбора информации о технологическом процессе, технологических установках, системах и ПО на предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах
		Примечание 1: Сбор информации может выполняться с использованием одной или более из перечисленных выше техник, пока нарушитель не получит достаточно информации для реализации другой тактики в продолжении атаки
T2	Получение первоначального доступа к компонентам систем и сетей Тактическая задача: нарушитель, находясь вне инфраструктуры сети или системы, стремится получить доступ к	T2.1. Использование внешних сервисов организации в сетях публичного доступа (Интернет) Примеры: 1) доступ к веб-серверу, расположенному в сети организации; 2) доступ к интерфейсу электронной почты OutlookWebAccess (OWA) почтового сервера организации
		T2.2. Использование устройств, датчиков, систем, расположенных на периметре или вне периметра физической защиты объекта, для получения первичного доступа к системам и компонентам внутри этого периметра.

Продолжение таблицы 11.1

№	Тактика	Основные техники
	любому узлу в инфраструктуре и использовать его как плацдарм для дальнейших действий	Примеры 1) доступ к датчикам автономной системы дистанционного контроля давления газа участка газопровода; 2) доступ к умному счетчику, расположенному на частном объекте, как к части инфраструктуры поставщика электроэнергии; 3) доступ к интерфейсу управления камеры видеонаблюдения через сети ближнего действия
		Т2.3. Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей для получения доступа к компонентам систем и сетей при удаленной атаке. Пример: обход межсетевого экрана путем эксплуатации уязвимостей реализации правил фильтрации
		Т2.4. Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию, для получения доступа к компонентам систем и сетей при удаленной атаке
		Т2.5. Эксплуатация уязвимостей компонентов систем и сетей при удаленной или локальной атаке. Примеры: 1) эксплуатация уязвимостей веб-сервера с целью выполнения произвольного кода в контексте этого сервера; 2) эксплуатация уязвимостей операционной системы устройства человеко-машинного интерфейса автоматизированной системы управления с целью внедрения средств получения вводимых на этом устройстве паролей доступа; 3) эксплуатация уязвимостей браузера вредоносными скриптами при посещении пользователем вредоносного или скомпрометированного веб-сайта
		Т2.6. Использование недокументированных возможностей программного обеспечения сервисов, приложений, оборудования, включая использование отладочных интерфейсов, программных, программно-аппаратных закладок
		Т2.7. Использование в системе внешних носителей информации, которые могли подключаться к другим системам и быть заражены вредоносным программным обеспечением. В том числе дарение, подмена или подлог носителей информации и внешних устройств, содержащих вредоносное программное обеспечение или предназначенных для реализации вредоносных функций. Примеры: 1) передача флеш-носителя в комплекте материалов выездного мероприятия; 2) подмена USB-адаптера беспроводной клавиатуры схожим внешне, но реализующим функции сбора и передачи данных устройством

Продолжение таблицы 11.1

№	Тактика	Основные техники
		Т2.8. Использование методов социальной инженерии, в том числе фишинга, для получения прав доступа к компонентам системы
		Т2.9. Несанкционированное подключение внешних устройств. Пример: несанкционированное подключение точки доступа Wi-Fi
		Т2.10. Несанкционированный доступ путем подбора учетных данных сотрудника или легитимного пользователя (методами прямого перебора, словарных атак, паролей производителей по умолчанию, использования одинаковых паролей для разных учетных записей, применения «радужных» таблиц или другими)
		Т2.11. Несанкционированный доступ путем компрометации учетных данных сотрудника организации, в том числе через компрометацию многократно используемого в различных системах пароля (для личных или служебных нужд)
		Т2.12. Использование доступа к системам и сетям, предоставленного сторонним организациям, в том числе через взлом инфраструктуры этих организаций, компрометацию личного оборудования сотрудников сторонних организаций, используемого для доступа. Пример: использование доступа третьей доверенной стороны (поставщики ИТ-услуг, поставщики услуг безопасности)
		Т2.13. Реализация атаки типа «человек посередине» для осуществления доступа, например, NTLM/SMB Relaying атаки
		Т2.14. Доступ путем эксплуатации недостатков систем биометрической аутентификации. Пример: демонстрация фотографии для аутентификации через функцию распознавания лиц
		Примечание 2: Получение доступа может выполняться в несколько шагов с использованием одной или более из перечисленных выше техник, пока нарушитель не достигнет целевой системы или не будет вынужден прибегнуть к другой тактике для продолжения атаки
Т3	Внедрение и исполнение вредоносного программного обеспечения в системах и сетях Тактическая задача: получив доступ к узлу сети или системы, нарушитель стремится внедрить в его	Т3.1. Автоматический запуск скриптов и исполняемых файлов в системе с использованием пользовательских или системных учетных данных, в том числе с использованием методов социальной инженерии
		Т3.2. Активация и выполнение вредоносного кода, внедренного в виде закладок в легитимное программное и программное-аппаратное обеспечение систем и сетей
		Т3.3. Автоматическая загрузка вредоносного кода с удаленного сайта или ресурса с последующим запуском на выполнение

Продолжение таблицы 11.1

№	Тактика	Основные техники
	программную среду инструментальные средства, необходимые ему для дальнейших действий	Т3.4. Копирование и запуск скриптов и исполняемых файлов через средства удаленного управления операционной системой и сервисами
		Т3.5. Эксплуатация уязвимостей типа удаленное исполнение программного кода (RCE, Remotecodeexecution)
		Т3.6. Автоматическое создание вредоносных скриптов при помощи доступного инструментария от имени пользователя в системе с использованием его учетных данных
		Т3.7. Подмена файлов легитимных программ и библиотек непосредственно в системе. *Примечание 3: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа ПО*
		Т3.8. Подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи. *Примечание 4: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа программного обеспечения*
		Т3.9. Подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления программного обеспечения, поставляемые производителем удаленно через сети связи, подмена информации о таких обновлениях, включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями. *Примечание 5: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа программного обеспечения*
		Т3.10. Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах *Примечание 6: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа программного обеспечения*
		Т3.11. Компрометация сертификата, используемого для цифровой подписи образа ПО, включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи (т.н. «даркверб») и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами

Продолжение таблицы 11.1

№	Тактика	Основные техники
		Т3.12. Компрометация средств создания программного кода приложений в инфраструктуре разработчика этих приложений (компиляторов, линковщиков, средств управления разработкой) для последующего автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы
		Т3.13. Компрометация средств сборки, конфигурирования и разворачивания программного кода, а также средств создания узкоспециализированного кода (к примеру, кода промышленных контроллеров) в инфраструктуре целевой системы для автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы
		Т3.14. Планирование запуска вредоносных программ при старте операционной системы путем эксплуатации стандартных механизмов, в том числе путем правки ключей реестра, отвечающих за автоматический запуск программ, запуска вредоносных программ как сервисов и т.п.
		Т3.15. Планирование запуска вредоносных программ через планировщиков задач в операционной системе, а также с использованием механизмов планирования выполнения в удаленной системе через удаленный вызов процедур. Выполнение в контексте планировщика в ряде случаев позволяет авторизовать вредоносное программное обеспечение и повысить доступные ему привилегии
		Т3.16. Запуск вредоносных программ при помощи легитимных, подписанных цифровой подписью утилит установки приложений и средств запуска скриптов (т.н. техника проксирования запуска), а также через средства запуска кода элементов управления ActiveX, компонентов фильтров (кодеков) и компонентов библиотек DLL. Примеры: 1) запуск MSI-файлов в операционной системе Windows при помощи утилиты msiexec; 2) использование утилит Regsvr32.exe (Microsoft Windows RegisterServer) и odbcconf.exe для проксирования исполнения кода библиотек dll в операционной системе Windows посредством внесения изменений в реестр операционных систем
		Примечание 7: Внедрение и исполнение вредоносного программного обеспечения в системах и сетях может выполняться в несколько шагов с использованием одной или более из перечисленных выше техник, пока нарушитель не достигнет целевой системы или не будет вынужден прибегнуть к другой тактике для продолжения атаки

Продолжение таблицы 11.1

№	Тактика	Основные техники
Т4	Закрепление (сохранение доступа) в системе или сети Тактическая задача: получив доступ к узлу сети с помощью некоторой последовательности действий, нарушитель стремится упростить себе повторное получение доступа к этому узлу, если он ему впоследствии понадобится (например, устанавливает средства удаленного управления узлом, изменяет настройки средств защиты и другие действия)	Т4.1. Несанкционированное создание учетных записей или кража существующих учетных данных
		Т4.2. Использование штатных средств удаленного доступа и управления операционной системы
		Т4.3. Скрытая установка и запуск средств удаленного доступа и управления операционной системы. Внесение изменений в конфигурацию и состав программных и программно-аппаратных средств атакуемой системы или сети, вследствие чего становится возможен многократный запуск вредоносного кода
		Т4.4. Маскирование подключенных устройств под легитимные (например, нанесение корпоративного логотипа, инвентарного номера, телефона службы поддержки)
		Т4.5. Внесение соответствующих записей в реестр, автозагрузку, планировщики заданий, обеспечивающих запуск вредоносного программного обеспечения при перезагрузке системы или сети
		Т4.6. Компрометация прошивок устройств с использованием уязвимостей или программно-аппаратных закладок, к примеру, внедрение новых функций в BIOS (UEFI), компрометация прошивок жестких дисков
		Т4.7. Резервное копирование вредоносного кода в областях, редко подвергаемых проверке, в том числе заражение резервных копий данных, сохранение образов в неразмеченных областях жестких дисков и сменных носителей
		Примечание 8: Закрепление (сохранение доступа в системе) может производиться с использованием одной или более из перечисленных выше техник
Т5	Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ Тактическая задача: внедрив вредоносное программное обеспечение или обеспечив	Т5.1. Удаленное управление через стандартные протоколы (например, RDP, SSH), а также использование инфраструктуры провайдеров средств удаленного администрирования. Пример: использование средств удаленного управления RMS/teamviewer для создания канала связи и управления скомпрометированной системой со стороны злоумышленников
		Т5.2. Использование штатных средств удаленного доступа и управления операционной системы
		Т5.3. Коммуникация с внешними серверами управления через хорошо известные порты на этих серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.)

Продолжение таблицы 11.1

№	Тактика	Основные техники
	постоянное присутствие на узле сети, нарушитель стремится автоматизировать управление внедренными инструментальными средствами, организовав взаимодействия скомпрометированным узлом и сервером управления, который может быть размещен в сети Интернет или в инфраструктуре организации	Т5.4. Коммуникация с внешними серверами управления через нестандартные порты на этих серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств
		Т5.5. Управление через съемные носители, в частности, передача команд управления между скомпрометированными изолированной системой и подключенной к Интернет системой через носители информации, используемые на обеих системах
		Т5.6. Проксирование трафика управления для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика управления во избежание обнаружения. Примеры: 1) использование скомпрометированных систем в той же сети, для которых правилами МЭ разрешен доступ в Интернет, в качестве прокси серверов; 2) использование инфраструктуры сети TOR для проксирования запросов к серверам управления; 3) использование одного коммуникационного протокола для запроса, и другого – для ответа на запрос
		Т5.7. Туннелирование трафика управления через VPN
		Т5.8. Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие
		Т5.9. Управление через подключенные устройства, реализующие дополнительный канал связи с внешними системами или между скомпрометированными системами в сети
		Т5.10. Использование средств обфускации, шифрования, стеганографии для сокрытия трафика управления
		Т5.11. Передача команд управления через нестандартно интерпретируемые типовые операции, к примеру, путем выполнения копирования файла по разрешенному протоколу (FTP или подобному), путем управления разделяемыми сетевыми ресурсами по протоколу SMB и т.п.
		Т5.12. Передача команд управления через публикацию на внешнем легитимном сервисе, таком как веб-сайт, облачный ресурс, ресурс в социальной сети и т.п.
		Т5.13. Динамическое изменение адресов серверов управления, идентификаторов внешних сервисов, на которых публикуются команды управления, и т.п. по известному алгоритму во избежание обнаружения

Продолжение таблицы 11.1

№	Тактика	Основные техники
		Примечание 9: Управление вредоносным программным обеспечением и (или) компонентами, к которым ранее был получен доступ, может производиться нарушителем с использованием одной или более из перечисленных выше техник для управления труднодоступными компонентами или для реализации резервных каналов управления
Т6	Повышение привилегий по доступу к компонентам систем и сетей Тактическая задача: получив первоначальный доступ к узлу с привилегиями, недостаточными для совершения нужных ему действий, нарушитель стремится повысить полученные привилегии и получить контроль над узлом	Т6.1. Получение данных для аутентификации и авторизации от имени привилегированной учетной записи путем поиска этих данных в папках и файлах, поиска в памяти или перехвата в сетевом трафике. Данные для авторизации включают пароли, хэш-суммы паролей, токены, идентификаторы сессии, криптографические ключи, но не ограничиваются ими
		Т6.2. Подбор пароля или другой информации для аутентификации от имени привилегированной учетной записи
		Т6.3 Эксплуатация уязвимостей ПО к повышению привилегий. Пример: эксплуатация уязвимости драйвера службы печати, позволяющей выполнить код с привилегиями системной учетной записи, через доступ к этому драйверу из приложения, запущенного от имени непривилегированного пользователя
		Т6.4. Эксплуатация уязвимостей механизма имперсонации (запуска операций в системе от имени другой учетной записи). Пример: эксплуатация уязвимости штатного механизма имперсонации, реализуемого операционной системой
		Т6.5. Манипуляции с идентификатором сессии, токеном доступа или иным параметром, определяющим права и полномочия пользователя в системе таким образом, что новый или измененный идентификатор/токен/параметр дает возможность выполнения ранее недоступных пользователю операций. Пример: кража и подделка cookie сессии для получения авторизованного доступа к веб-интерфейсу управления сетевого устройства
		Т6.6. Обход политики ограничения пользовательских учетных записей в выполнении групп операций, требующих привилегированного режима. Пример: обход UserAccountControl в операционной системе Windows
		Т6.7. Использование уязвимостей конфигурации системы, служб и приложений, в том числе предварительно сконфигурированных профилей привилегированных пользователей, автоматически запускаемых от имени привилегированных пользователей скриптов, приложений и экземпляров окружения, позволяющих вредоносному ПО выполняться с

Продолжение таблицы 11.1

№	Тактика	Основные техники
		повышенными привилегиями. Примеры: 1) использование профилей PowerShell для закрепления вредоносного ПО в системе и выполнения этого ПО с повышенными привилегиями; 2) конфигурация команды перехода в привилегированный режим sudo, при которой успешный результат выполнения этой команды на некоторое время кэшируется, что при определенных обстоятельствах может быть использовано вредоносным кодом для выполнения привилегированных операций в течение этого времени; 3) параметры исполнения файлов (ImageFileExecutionOptions, IFEO), позволяющие переключать исполнение файлов в режим отладки, выполняя вредоносные приложения под видом отладчиков и средств мониторинга, что позволяет им отключать системные приложения и средства защиты
		Т6.8. Эксплуатация уязвимостей, связанных с отдельным, и вероятно менее строгим контролем доступа к некоторым ресурсам (например, к файловой системе) для непривилегированных учетных записей. Пример: подмена на диске бинарных файлов или скриптов, предназначенных для исполнения в привилегированном контексте, приложением, исполняющимся в непривилегированном контексте
		Т6.9. Эксплуатация уязвимостей средств ограничения среды исполнения (виртуальные машины, песочницы и т.п.) для исполнения кода вне этой среды. Пример: эксплуатация уязвимости обработки буфера данных в рамках песочницы, реализуемой браузером для ограничения работы мобильного кода (Javascript), с последующим выполнением кода в контексте процесса браузера
		Примечание 10: Повышение привилегий по доступу к компонентам систем и сетей может производиться с использованием одной или более из перечисленных выше техник, пока нарушитель не получит достаточно привилегий для реализации другой тактики в продолжении атаки
Т7	Сокрытие действий и применяемых при этом средств от обнаружения Тактическая задача: нарушитель стремится затруднить применение	Т7.1. Использование нарушителем или вредоносной платформой штатных инструментов администрирования, утилит и сервисов операционной системы, сторонних утилит, в том числе двойного назначения. Пример: использование популярной утилиты PsExec для ОС Windows как администраторами, так и нарушителями

Продолжение таблицы 11.1

№	Тактика	Основные техники
	мер защиты информации, которые способны помешать его действиям или обнаружить их	Т7.2. Очистка/затирание истории команд и журналов регистрации, перенаправление записей в журналы регистрации, переполнение истории команд и журналов регистрации, затруднение доступа к журналам регистрации для авторизованных пользователей
		Т7.3. Удаление файлов, переписывание файлов произвольными данными, форматирование съемных носителей
		Т7.4. Отключение средств защиты от угроз информационной безопасности, в том числе средств антивирусной защиты, механизмов аудита, консолей оператора мониторинга и средств защиты других типов
		Т7.5. Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса
		Т7.6. Подделка данных вывода средств защиты от угроз информационной безопасности
		Т7.7. Подделка данных телеметрии, данных вывода автоматизированных систем управления, данных систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса, данных видеонаблюдения и других визуально или автоматически интерпретируемых данных
		Т7.8. Выполнение атаки отказа в обслуживании на основные и резервные каналы связи, которые могут использоваться для доставки сообщений о неработоспособности систем или их компонентов или о других признаках атаки
		Т7.9. Подписание кода, включая использование скомпрометированных сертификатов авторитетных производителей ПО для подписания вредоносных программных модулей. *Примечание 11: Сочетается с техникой компрометации сертификата, используемого для цифровой подписи образа ПО*
		Т7.10. Внедрение вредоносного кода в доверенные процессы операционной системы и другие объекты, которые не подвергаются анализу на наличие такого кода, для предотвращения обнаружения
		Т7.11. Модификация модулей и конфигурации вредоносного программного обеспечения для затруднения его обнаружения в системе.

Продолжение таблицы 11.1

№	Тактика	Основные техники
		Пример: внесение изменений в модули и конфигурацию вредоносного ПО для удаления индикаторов компрометации этим ВПО после обнаружения его в других системах
		Т7.12. Манипуляции именами и параметрами запуска процессов и приложений для обеспечения скрытности. Примеры: 1) сокрытие окна приложения через параметры запуска процесса в ОС Windows; 2) выбор для вредоносного приложения имени файла (процесса), похожего на имя известного и/или системного приложения или совпадающего с ним
		Т7.13. Создание скрытых файлов, скрытых учетных записей
		Т7.14. Установление ложных доверенных отношений, в том числе установка корневых сертификатов для успешной валидации вредоносных программных модулей и авторизации внешних сервисов
		Т7.15. Внедрение вредоносного кода выборочным/целевым образом на наиболее важные системы или системы, удовлетворяющие определенным критериям, во избежание преждевременной компрометации информации об используемых при атаке уязвимостях и обнаружения факта атаки
		Т7.16. Искусственное временное ограничение распространения или активации вредоносного кода внутри сети, во избежание преждевременного обнаружения факта атаки. Пример: распространение вредоносного ПО единовременно по всем интересующим злоумышленникам системам и единовременный запуск его на выполнение по команде, вплоть до выполнения которой компрометацию системы обнаружить сложно
		Т7.17. Обфускация, шифрование, упаковка с защитой паролем или сокрытие стеганографическими методами программного кода вредоносного ПО, данных и команд управляющего трафика, в том числе при хранении этого кода и данных в атакуемой системе, при хранении на сетевом ресурсе или при передаче по сети
		Т7.18. Использование средств виртуализации для сокрытия вредоносного кода или вредоносной активности от средств обнаружения в операционной системе
		Т7.19. Туннелирование трафика управления через VPN
		Т7.20. Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие

Продолжение таблицы 11.1

№	Тактика	Основные техники
		Т7.21. Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами
		Т7.22. Подмена и компрометация прошивок, в том числе прошивок BIOS, жестких дисков
		Т7.23. Подмена файлов легитимных программ и библиотек непосредственно в системе. *Примечание 12: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа ПО*
		Т7.24. Подмена легитимных программ и библиотек, а также легитимных обновлений программного обеспечения, поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи. *Примечание 13: В том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа ПО*
		Т7.25. Подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления программного обеспечения, поставляемые производителем удаленно через сети связи, информации о таких обновлениях, включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями. *Примечание 14: в том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа ПО*
		Т7.26. Подмена дистрибутивов (установочных комплектов) программ на носителях информации или общих сетевых ресурсах. *Примечание 15: в том числе может сочетаться с техникой компрометации сертификата, используемого для цифровой подписи образа ПО*
		Т7.27. Компрометация сертификата, используемого для цифровой подписи образа ПО, включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи (т.н. «дарквеб») и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами
		Т7.28. Компрометация средств создания программного кода приложений в инфраструктуре разработчика этих приложений (компиляторов, линковщиков, средств управления разработкой) для последующего автоматизированного внесения изменений в этот код,

Продолжение таблицы 11.1

№	Тактика	Основные техники
		устанавливаемый авторизованным пользователем на целевые для нарушителя системы
		Т7.29. Компрометация средств сборки, конфигурирования и разворачивания программного кода, а также средств создания узкоспециализированного кода (к примеру, кода промышленных контроллеров), в инфраструктуре целевой системы, для автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы
		Примечание 16: Сокрытие действий и применяемых при этом средств от обнаружения может производиться с использованием одной или более из перечисленных выше техник для сокрытия разных свидетельств компрометации системы или для более эффективного сокрытия
Т8	Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям Тактическая задача: получив доступ к некоторым узлам инфраструктуры, нарушитель стремится получить доступ к другим узлам. Подобное распространение доступа может быть нецеленаправленным: так, еще не зная, к каким именно компонентам инфраструктуры требуется получить доступ для того, чтобы вызвать нужные ему негативные последствия, нарушитель может стремиться получить контроль над как можно большей частью инфраструктуры систем и сетей	Т8.1. Эксплуатация уязвимостей для повышения привилегий в системе или сети для удаленного выполнения программного кода для распространения доступа
		Т8.2. Использование средств и интерфейсов удаленного управления для получения доступа к смежным системам и сетям
		Т8.3. Использование механизмов дистанционной установки программного обеспечения и конфигурирования. Пример: распространение вредоносного кода групповыми политиками ActiveDirectory, обычно используемыми для автоматического управления легитимным программным обеспечением
		Т8.4. Удаленное копирование файлов, включая модули вредоносного программного обеспечения и легитимные программные средства, которые позволяют злоумышленнику получать доступ к смежным системам и сетям
		Т8.5. Изменение конфигурации сети, включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами
		Т8.6. Копирование вредоносного кода на съемные носители
		Т8.7. Размещение вредоносных программных модулей на разделяемых сетевых ресурсах в сети
		Т8.8. Использование доверенных отношений скомпрометированной системы и пользователей этой системы с другими системами и пользователями для распространения вредоносного программного обеспечения или для доступа к системам и информации в других

Продолжение таблицы 11.1

№	Тактика	Основные техники
		системах и сетях. Пример: отсылка сообщений корпоративной электронной почты от имени коллег и прочих доверенных лиц
		Примечание 17: Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям может выполняться в несколько шагов с использованием одной или более из перечисленных выше техник, пока нарушитель не достигнет целевой системы или не будет вынужден прибегнуть к другой тактике для продолжения атаки
Т9	Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз Тактическая задача: в ходе реализации угроз безопасности информации, нарушителю может потребоваться получить и вывести за пределы инфраструктуры большие объемы информации, избежав при этом обнаружения или противодействия	Т9.1. Доступ к системе для сбора информации и вывод информации через стандартные протоколы управления (например, RDP, SSH), а также использование инфраструктуры провайдеров средств удаленного администрирования. Пример: использование средств удаленного управления RMS / teamviewer для создания канала связи и управления скомпрометированной системой со стороны злоумышленников
		Т9.2. Доступ к системе для сбора информации и вывод информации через использование штатных средств удаленного доступа и управления операционной системы
		Т9.3. Вывод информации на хорошо известные порты на внешних серверах, разрешенные на межсетевом экране (SMTP/25, HTTP/80, HTTPS/443 и др.)
		Т9.4. Вывод информации на нестандартные порты на внешних серверах, что в некоторых случаях позволяет эксплуатировать уязвимости средств сетевой фильтрации для обхода этих средств
		Т9.5. Отправка данных по известным протоколам управления и передачи данных
		Т9.6. Отправка данных по собственным протоколам
		Т9.7. Проксирование трафика передачи данных для маскировки подозрительной сетевой активности, обхода правил на межсетевом экране и сокрытия адресов инфраструктуры нарушителей, дублирование каналов связи, обфускация и разделение трафика передачи данных во избежание обнаружения. Примеры: 1) использование скомпрометированных систем в той же сети, для которых правилами МЭ разрешен доступ в Интернет в качестве прокси серверов; 2) использование инфраструктуры сети TOR для проксирования запросов к серверам управления; 3) использование одного коммуникационного протокола для запроса, и другого – для ответа на запрос
		Т9.8. Туннелирование трафика передачи данных через VPN

Продолжение таблицы 11.1

№	Тактика	Основные техники
		Т9.9. Туннелирование трафика управления в поля заполнения и данных служебных протоколов, к примеру, туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие
		Т9.10. Вывод информации через съемные носители, в частности, передача данных между скомпрометированными изолированной системой и подключенной к Интернет системой через носители информации, используемые на обеих системах
		Т9.11. Отправка данных через альтернативную среду передачи данных. Пример: вывод конфиденциальной информации через субтитры видеоряда, демонстрируемого на веб-сайте
		Т9.12. Шифрование выводимой информации, использование стеганографии для сокрытия факта вывода информации
		Т9.13. Вывод информации через предоставление доступа к файловым хранилищам и базам данных в инфраструктуре скомпрометированной системы или сети, в том числе путем создания новых учетных записей или передачи данных для аутентификации и авторизации имеющихся учетных записей
		Т9.14. Вывод информации путем размещения сообщений или файлов на публичных ресурсах, доступных для анонимного нарушителя (форумы, файлообменные сервисы, фотобанки, облачные сервисы, социальные сети)
		Примечание 18: Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз может выполняться с использованием одной или более из перечисленных выше техник для реализации резервных каналов вывода информации
Т10	Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям Тактическая задача: достижение нарушителем конечной цели,	Т10.1. Несанкционированный доступ к информации в памяти системы, файловой системе, базах данных, репозиториях, в программных модулях и прошивках
		Т10.2. Несанкционированное воздействие на системное программное обеспечение, его конфигурацию и параметры доступа
		Т10.3. Несанкционированное воздействие на программные модули прикладного программного обеспечения
		Т10.4. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прикладного программного обеспечения
		Т10.5. Несанкционированное воздействие на программный код, конфигурацию и параметры

Продолжение таблицы 11.1

№	Тактика	Основные техники
	приводящее к реализации моделируемой угрозы и причинению недопустимых негативных последствий	доступа системного программного обеспечения
		Т10.6. Несанкционированное воздействие на программный код, конфигурацию и параметры доступа прошивки устройства
		Т10.7. Подмена информации (например, платежных реквизитов) в памяти или информации, хранимой в виде файлов, информации в базах данных и репозиториях, информации на неразмеченных областях дисков и сменных носителей
		Т10.8. Уничтожение информации, включая информацию, хранимую в виде файлов, информацию в базах данных и репозиториях, информацию на неразмеченных областях дисков и сменных носителей
		Т10.9. Добавление информации (например, дефейсинг корпоративного портала, публикация ложной новости)
		Т10.10. Организация отказа в обслуживании одной или нескольких систем, компонентов системы или сети
		Т10.11. Нецелевое использование ресурсов системы. Примеры: 1) организация майнинговой платформы; 2) организация платформы для осуществления атак отказа в обслуживании на смежные системы и сети.
		Т10.12. Несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или нарушения функций управления, в том числе на АСУ критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов. Примеры: 1) воздействие на автоматизированные системы управления объектов транспорта; 2) удаленное воздействие на цифровые системы и первичное оборудование объектов электроэнергетики; 3) воздействие на системы управления технологическим процессом нефтехимического объекта
		Т10.13. Несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или поломки оборудования, в том числе АСУ критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов

Окончание таблицы 11.1

№	Тактика	Основные техники
		Т10.14. Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности, в том числе критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов
		Т10.15. Воздействие на информационные ресурсы через системы распознавания визуальных, звуковых образов, системы геопозиционирования и ориентации, датчики вибрации, прочие датчики и системы преобразования сигналов физического мира в цифровое представление с целью полного или частичного вывода системы из строя или несанкционированного управления системой. Примеры: 1) нанесение нелегитимной разметки дорожного полотна с целью вызова сбоя системы автоматического управления автомобилем; 2) использование специальных символов в идентификационном знаке физического объекта, распознаваемом камерами видеонаблюдения
		Примечание 19: Несанкционированный доступ и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящее к негативным последствиям при реализации угроз безопасности информации или реализации новых угроз, может выполняться с использованием одной или более из перечисленных выше техник для повышения эффективности воздействия с точки зрения нарушителя или для реализации нескольких типов воздействия на атакуемую систему

Формат 60×90/8. Усл.печ.л. 10,38
Зак.