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

**Определение источников угроз безопасности информации**

Определение возможных актуальных нарушителей

Исходные данные:

1. 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;
2. б) описания векторов компьютерных атак, содержащихся в базах данных и иных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.);
3. 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;
4. 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);
5. 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);
6. е) результаты оценки ущерба (рисков), проведенной обладателем информации или оператором;
7. ж) негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с настоящей Методикой;
8. 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

Виды нарушителей:

* 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.

Результаты:

1. а) виды актуальных нарушителей и возможные цели реализации ими угроз безопасности информации, а также их возможности;
2. б) категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы

**Оценка способов реализации (возникновения) угроз безопасности информации**

Исходные данные:

1. 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;
2. б) описания векторов компьютерных атак, содержащихся в базах данных и иных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.);
3. 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);
4. г) негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с настоящей Методикой;
5. д) объекты воздействия угроз безопасности информации и соответствующие им виды воздействия, определенные в соответствии с настоящей Методикой;
6. 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.

Способы реализации угроз:

* 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, программноаппаратных 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.

Результат:

1. а) виды и категории нарушителей, которые имеют возможность использования актуальных способов;
2. б) актуальные способы реализации угроз безопасности информации и типы интерфейсов объектов воздействия, за счет которых они могут быть реализованы.

**Оценка актуальности угроз безопасности информации**

Исходные данные:

1. 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;
2. 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.);
3. в) негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в соответствии с настоящей Методикой;
4. г) объекты воздействия угроз безопасности информации и виды воздействий на них, определенные в соответствии с настоящей Методикой;
5. 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;
6. е) актуальные способы реализации (возникновения) угроз безопасности информации.