Данный материал является фрагментом электронного учебника
по информационной безопасности и может обновляться.
При цитировании рекомендуется использовать ссылку:

Амелин Р. В. Информационная безопасность. Конспект лекций // Амелин Р.В. Лаборатория преподавателя [Электронный ресурс]. URL: rv-lab.ru (2017).

Лекция 6. Угрозы информационной безопасности

6.1. Виды угроз информационной безопасности

Угроза – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Соответственно *угрозой информационной безопасности* называется потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию или компоненты АИС может прямо или косвенно привести к нанесению ущерба интересам субъектов информационных отношений.

Уязвимость – недостаток в программном обеспечении, оборудовании или процедуре, который порождает угрозу. Уязвимость – это отсутствие или слабость защитных мер.

Атака – попытка реализации угрозы.

Нарушение – реализация угрозы.

Определение, анализ и классификация возможных угроз безопасности АИС является одним из важнейших аспектов проблемы обеспечения ее безопасности. Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для проведения анализа риска и формулирования требований к системе защиты.

Классификацию угроз ИБ можно выполнить по нескольким критериям:

1. По свойству информации, подвергающемуся угрозе:
   - Угрозы конфиденциальности;
   - Угрозы целостности;
   - Угрозы доступности;
   - Угрозы апеллируемости (возникают, когда легальный пользователь отрицает свои действия по передаче или приему информации, чтобы снять с себя ответственность).
2. По компонентам АИС, на которые нацелена угроза:
   - Данные;
   - Программное обеспечение;
   - Аппаратное обеспечение;
   - Поддерживающая инфраструктура.
3. По расположению источника угроз:
   - Внешние угрозы
   - Внутренние угрозы (угрозы со стороны инсайдеров являются наиболее опасными).
4. По природе возникновения:
   - *Естественные угрозы* – это угрозы, вызванные воздействиями на АИС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.
   - *Искусственные угрозы* – угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить *непреднамеренные* (неумышленные, случайные) угрозы, вызванные ошибками в проектировании

АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п., и *преднамеренные* (умышленные) угрозы, связанные с целенаправленными устремлениями злоумышленников.

Компания Microsoft рекомендует систему категоризации угроз под названием *STRIDE*. Эта мнемоника означает шесть категорий угроз, на которые предлагается проверить каждый компонент информационной системы – желательно, еще на этапе проектирования. Конечно, безопасность каждого отдельного компонента еще не означает безопасности системы в целом, но если один из компонентов оказывается подвержен угрозе, то система в целом также не безопасна. По сути, это классификация первого типа: каждой угрозе соответствует некоторое свойство информационной безопасности, которое нарушается при успешной атаке:

Spoofing (подмена данных) – может ли кто-то или что-то обмануть механизмы проверки подлинности, т.е. *аутентификации*.

Tampering (изменение данных) – нарушение *целостности*.

Repudiation (аннулирование) – может ли пользователь успешно отрицать совершенные им нелегальные действия; нарушение *апеллируемости*.

Information Disclosure (раскрытие информации) – нарушение *конфиденциальности*.

Denial of Service (отказ в обслуживании) – нарушение *доступности*.

Elevation of privilege (повышение прав доступа) – может ли пользователь в нарушение процедуры *авторизации* получить доступ к информации или функционалу, для которых он не имеет полномочий.

Самостоятельная работа. Рассмотрев приведенный ниже перечень конкретных угроз (приведенный в учебнике В.Ю. Гайковича и Д.В. Ершова[1]), классифицируйте каждую из них по четырем приведенным выше критериям.

Например: *ввод ошибочных данных – угроза целостности, нацелена на данные, внутренняя, искусственная непреднамеренная.*

Примечание: смысл выполнения задания заключается не в выполнении собственно классификации (которая зачастую достаточно очевидна). Выполняя это задание, студент волей-неволей должен *осознать* каждую из угроз (а не просто мельком просмотреть список) и, таким образом, получить представление о проблематике информационной безопасности.

1. Неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);
2. Неправомерное отключение оборудования или изменение режимов работы устройств и программ;

[1] Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий. — М.: МИФИ, 1995.

3. Неумышленная порча носителей информации;
4. Запуск программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование носителей информации, удаление данных и т.п.);
5. Нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
6. Заражение компьютера вирусами;
7. Неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;
8. Разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
9. Проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;
10. Игнорирование организационных ограничений (установленных правил) при работе в системе;
11. Вход в систему в обход средств защиты (загрузка посторонней операционной системы с внешних носителей и т.п.);
12. Некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
13. Пересылка данных по ошибочному адресу абонента (устройства);
14. Ввод ошибочных данных;
15. Неумышленное повреждение каналов связи.
16. Физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);
17. Отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
18. Действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);
19. Внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);
20. Вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;

21. Применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;
22. Перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.);
23. Перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;
24. Хищение носителей информации;
25. Несанкционированное копирование носителей информации;
26. Хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
27. Чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
28. Чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме используя недостатки операционных систем и других приложений;
29. Незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»);
30. Несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;
31. Вскрытие шифров криптозащиты информации;
32. Внедрение аппаратных спецвложений, программных «закладок» и вирусов (троянских коней), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;
33. Незаконное подключение к линиям связи с целью работы «между строк», с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;
34. Незаконное подключение к линиям связи с целью подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

6.2. Модель угроз информационной безопасности

Управление безопасностью базируется на четко идентифицированных и оцененных активах компании (Харрис, 2011). После того как такие активы выявлены, в соответствии с их ценностью, разрабатываются меры по обеспечению их конфиденциальности, целостности и доступности, то есть, меры по защите этих активов. Но сначала необходимо определить, *от чего их требуется защищать*.

В теории рисков для определения *меры риска* используется формула $R = P \cdot C$, где P – вероятность наступления нежелательного события, а C – ущерб от наступления такого события. Застраховаться от всех угроз на свете невозможно, но можно выделить наиболее вероятные и наиболее критичные по своим последствиям угрозы. Другими словами, принимать во внимание, тратить силы и средства следует на борьбу с такими рисками, для которых величина R значительна. Очевидно, что та же самая логика справедлива и в отношении угроз информационной безопасности.

Одни и те же угрозы могут иметь разную меру риска, когда речь идет о различной информации, принадлежащей различным людям и организациям. Сравним, к примеру, меру риска DDoS-атаки, если она направлена на:

а) персональный сайт автора этого учебника;

б) сайт английского букмекера, предназначенный для приема ставок (накануне проведения скачек на Золотой кубок в Аскоте);

в) региональный сайт МЧС, предназначенный для информирования населения о чрезвычайных ситуациях (в разгар сложной пожарной обстановки в регионе).

Очевидно, что ущерб от успешной реализации такой атаки будет весьма различаться. Также будет различаться вероятность реализации такой угрозы как «доступ к защищаемой информации с использованием средств радиоэлектронной разведки», если речь идет о:

а) личном дневнике школьницы Маши;

б) списке рекламодателей газеты «Степной путь»;

в) сведений о засекреченной сделке по поглощению крупной корпорации.

Для построения адекватной системы защиты, необходимо выявить *актуальные* угрозы информационной безопасности конкретной защищаемой информации, то есть, угрозы с существенной мерой риска.

В одном из исследований Минкомсвязи России актуальность угрозы предлагается рассчитывать по следующей таблице[2]:

Реализуемость угрозы	**Показатель опасности угрозы**		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

[2] Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли // [Электронный ресурс]. URL: http://minsvyaz.ru/common/upload/publication/1410065MC.pdf (дата обращения: 21.04.2013).

Microsoft предлагает свою методику оценки угроз, которая называется *DREAD*. Для каждой угрозы оцениваются пять параметров (по шкале от 0 до 3):

Damage – опасность – насколько велик ущерб от реализации угрозы.

Reproducibility – воспроизводимость – насколько легко повторить атаку (если для повтора атаки требуется редкое стечение обстоятельств, параметр будет низким).

Exploitability – насколько большие усилия нужны для осуществления атаки.

Affected users – как много пользователей пострадает в результате реализации угрозы.

Discoverability – насколько легко обнаружить уязвимость, приводящую к угрозе.

Значения этих пяти параметров складываются и получается относительный рейтинг угрозы: **Risk = (D + R + E + A + D) / 5**. При построении системы защиты приоритет отдается борьбе с угрозами, занимающими более высокие места в рейтинге.

Методику DREAD рекомендуется использовать в совокупности с моделью STRIDE.

Как показано выше, у различных информационных систем (а также объектов одной информационной системы) может быть различный набор актуальных угроз, следовательно, понадобятся и различные меры защиты.

Описание существующих угроз с указанием их актуальности (возможности реализации и последствий) называется ***моделью угроз информационной безопасности***.

Приведем определение модели угроз, закрепленное в нормативном документе.

- Модель угроз информационной безопасности – это описание источников угроз ИБ; методов реализации угроз ИБ; объектов, пригодных для реализации угроз ИБ; уязвимостей, используемых источниками угроз ИБ; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштаба потенциального ущерба[3].

Этапы построения модели угроз:

1. Выявление критических объектов информационной системы. Это может быть как информация, так и программно-аппаратные компоненты, которые нуждаются в защите.

2. Выявление источников угроз. Источником угрозы может быть человек (нарушитель), материальный объект или физическое явление. Подробнее этот этап рассматривается в следующем параграфе.

3. Построение перечня возможных угроз для каждого критического объекта с указанием способа их реализации и оценкой реализуемости (низкая, средняя, высокая или очень высокая).

4. Оценка материального ущерба и других возможных последствий угроз. Выявление актуальных угроз.

При разработке системы безопасности необходимо предусмотреть *меры противодействия* каждой из актуальных угроз (таким образом, чтобы эти угрозы перешли в разряд неактуальных из-за низкой реализуемости в защищенной системе).

---

[3] Стандарт ЦБ РФ СТО БР ИББС-1.0-2010 «Обеспечение ИБ организаций банковской системы РФ. Общие положения». Принят и введен в действие Распоряжением Банка России от 21 июня 2010 года №Р705.

В последнее время практически каждой организации приходится заниматься разработкой модели угроз. Любая организация обязана вести как минимум бухгалтерский учет, в процессе которого (при начислении заработной платы, исчислении налогов и т.д.) обрабатываются персональные данные сотрудников. Федеральный закон «О персональных данных» возлагает на оператора персональных данных (а это та самая организация и есть) обеспечение их конфиденциальности. Таким образом, у организации есть как минимум один информационный актив, который необходимо защищать. И даже если вышеописанные угрозы так и останутся нереализованными, за ненадлежащую систему защиты персональных данных организация может быть наказана контролирующими органами.

Для таких организаций (которым кроме персональных данных сотрудников и защищать-то особенно нечего, а поэтому специалиста по информационной безопасности они не держат) существует методический нормативный документ – *базовая модель угроз*[4]. Эта обобщенная модель может использоваться для разработки частной модели угроз безопасности персональных данных в конкретных информационных системах с учетом их назначения, условий и особенностей функционирования.

Существуют программы, которые составляют модель угроз информационной безопасности на основе анкеты. Такие программы могут сильно облегчить рутинную работу специалисту по автоматизации и внедрению систем защиты, но неопытным пользователям (не имеющим достаточной квалификации в сфере информационной безопасности) полагаться на такие программы не стоит. В качестве примера можно привести разработку Wingdoc ПД для системы персональных данных (рис. 6.1).

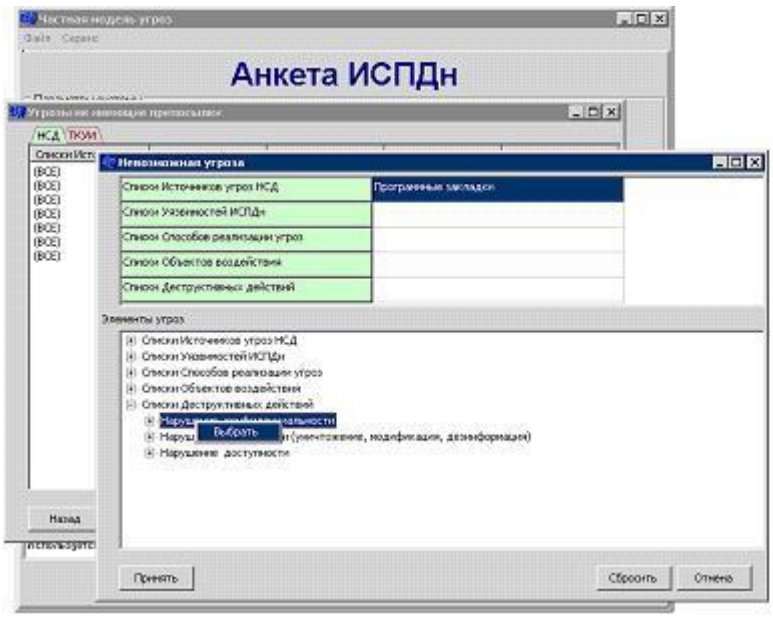

Рис. 6.1. Окно программы Wingdoc ПД

[4] Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена решением ФСТЭК России от 15 февраля 2008 г.

6.3 Модель нарушителя

Нарушитель информационной безопасности – физическое лицо, случайно или преднамеренно совершающий действия, следствием которых является нарушение информационной безопасности (конфиденциальности, целостности или доступности информации). Другими словами, нарушитель – это лицо, осуществляющее попытку выполнения запрещенных операций с данными. ***Злоумышленником*** называют нарушителя, который предпринимает такую попытку намеренно и, как правило, из корыстного интереса

Чтобы построить качественную модель угроз, необходимо иметь представление о возможных нарушителях информационной безопасности, поскольку искусственные угрозы (особенно преднамеренные) являются наиболее опасными. Для этого предварительно создается ***модель нарушителя информационной безопасности***. Она состоит из профилей (описаний) вероятных нарушителей, каждый из которых включает следующие предположения:

1. Категория лиц, к которым может принадлежать нарушитель.

- Внешние нарушители. Бывшие сотрудники предприятия, клиенты, посетители, конкуренты, случайные лица, преступные группировки.
- Внутренние нарушители (инсайдеры). Более опасная категория. Включает пользователей системы, обслуживающий персонал, разработчиков АИС, сотрудников службы безопасности, руководителей и т.д.

2. Мотивы нарушителя:

- безответственность (нарушения вызываются некомпетентностью или небрежностью без наличия злого умысла);
- самоутверждение (получая доступ к запретным данным, нарушитель растет в своих глазах или глазах коллег; свои действия часто воспринимает как игру);
- корыстный интерес.

3. Уровень знаний нарушителя (в контексте анализируемой системы):

- пользователь;
- администратор;
- программист;
- специалист в области информационной безопасности.

4. Возможности нарушителя (используемые методы и средства):

- может получать сведения только от других лиц;
- использует штатные средства доступа к данным (возможно, в несанкционированном режиме);
- пассивный перехват;
- активный перехват (возможность модификации данных).

5. Время действия:

- во время функционирования информационной системы;
- во время простоя системы;
- в любое время.

6. Место действия:

- без доступа на контролируемую территорию организации;
- с доступом на контролируемую территорию (но без доступа к техническим средствам);
- с рабочих мест пользователей;
- с доступом к базам данных АИС;
- с доступом к подсистеме защиты АИС.

Создавая модель нарушителя, можно опираться на шаблоны и методические рекомендации, специально разработанные для конкретной отрасли. Например, в отрасли связи принят нормативный документ, описывающий типовую модель нарушителя (конкретное предприятие может дорабатывать ее с учетом своей специфики). В этой модели внутренние нарушители подразделяются на восемь категорий, причем с каждой категорией соотнесены возможности нарушителя. Приведем фрагмент этой модели:

«К седьмой группе относятся лица из числа программистов-разработчиков сторонней организации, являющихся поставщиками ПО и лица, обеспечивающие его сопровождение на объекте размещения ИСПДн (информационной системы персональных данных).

Лицо данной группы:

− обладает информацией об алгоритмах и программах обработки информации в ИСПДн;

− обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в ПО ИСПДн на стадии его разработки, внедрения и сопровождения;

− может располагать любыми фрагментами информации о ТС обработки и защиты информации в ИСПДн»[5].

[5] Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли. Решение секции №1 Научно-технического совета Минкомсвязи России «Научно-техническое и стратегическое развитие отрасли» от 21 апреля 2010 года № 2 // URL: http://minsvyaz.ru/common/upload/publication/1410065MC.pdf