Классы угроз информационной безопасности

Доклад по дисциплине 'Информационная безопасность'

Манаева Варвара Евгеньевна, НФИбд-01-20

Содержание

1 Актуальность

Информация во все времена была важным аспектом жизни людей. В любом моменте истории нашей цивилизации можно найти моменты, когда информация влияла на жизни групп, деревень, городов и стран. Будь то информация о новом способе обработки какого-то материала для ремесленников и творцов, или сведения о научных изысканиях других, или информация о партнёрах и клиентах потенциальных и не только конкурентов — информация всегда может помочь (или навредить) людям.

Именно из-за своей ценности в жизни людей информация подвергается посягательствам со стороны различных мошенников. Риски существуют как на уровне физических и/или юридических лиц, так и на государственном уровне. Игнорирование возникающих проблем приводит к потере конкурентоспособности, снижению репутации, увеличению недоверия и многим другим социальным последствиям для пострадших.

Актуальность угроз целостности и конфиденциальности информации требует внимательного отношения к задаче ее защиты. 20 лет назад задача обеспечения безопасности информации решалась при помощи средств криптографической защиты, установления межсетевых экранов, разграничения доступа. Сейчас этих технологий недостаточно. Любая информация, имеющая финансовую, конкурентную, военную или политическую ценность, подвергается угрозе. Дополнительным риском становится возможность перехвата управления критическими объектами информационной инфраструктуры, в частности, правительственной информацией.

За первые 7 месяцев 2023 года количество преступлений в сфере компьютерной информации возрасло на $173,9$ по сравнению с аналогичным периодом 2022 [1,2] Проблемой становится то, что с ростом числа нарушений снижается их раскрываемость. По статистике генпрокураторы ещё в 2020 году она не превышала 25. После же пандемии и вовсе количество преступлений неумолимо растёт, а количество людей, способных бороться с преступлениями в сфере информационнй безопасности, — падает.

Для понимания как защищать целостность, конфиденциальность и доступность информации, необходимо понимать, как происходят их нарушения. Необходимость классификации угроз ИБ обусловлена тем, что архитектура современных средств автоматизированной обработки информации, организационное, структурное и функциональное построение информационно-вычислительных систем и сетей, технологии и условия автоматизированной обработки информации такие, что накапливаемая, хранимая и обрабатываемая информация подвержена случайным влияниям чрезвычайно большого числа факторов, в силу чего становится невозможным формализовать задачу описания полного множества угроз. Как следствие, для защищаемой системы определяют не полный перечень угроз, а перечень классов угроз.

2 Цель работы

Продемонстрировать классификации угроз информационной безопасности для большего понимания их людьми.

3 Теоретическое введение [3]

3.1 Информационная безопасность

Информационная безопасность (англ. Information Security, а также — англ. InfoSec) — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая). Основная задача информационной безопасности — сбалансированная защита конфиденциальности, целостности и доступности данных, с учётом целесообразности применения и без какого-либо ущерба производительности организации.

Выделяют следующие принципы инфорационной безопасности:

- **Целостность** информационных данных означает способность информации сохранять изначальный вид и структуру как в процессе хранения, как и после неоднократной передачи. Вносить изменения, удалять или дополнять информацию вправе только владелец или пользователь с легальным доступом к данным.
- **Конфиденциальность** – характеристика, которая указывает на необходимость ограничить доступа к информационным ресурсам для определенного круга лиц. В процессе действий и операций информация становится доступной только пользователям, который включены в информационные системы и успешно прошли идентификацию.

- **Доступность** информационных ресурсов означает, что информация, которая находится в свободном доступе, должна предоставляться полноправным пользователям ресурсов своевременно и беспрепятственно.
- **Достоверность** указывает на принадлежность информации доверенному лицу или владельцу, который одновременно выступает в роли источника информации.

Системный подход к описанию информационной безопасности предлагает выделить следующие составляющие информационной безопасности:

1. Законодательная, нормативно-правовая и научная база;
2. Структура и задачи органов (подразделений), обеспечивающих безопасность ИТ;
3. Организационно-технические и режимные меры и методы (Политика информационной безопасности);
4. Программно-технические способы и средства обеспечения информационной безопасности.

3.2 Угроза информационной безопасности

Угрозой информации называют потенциально возможное влияние или воздействие на автоматизированную систему с последующим нанесением убытка чьим-то потребностям.

На сегодня существует более 100 позиций и разновидностей угроз информационной системе. Важно проанализировать все риски с помощью разных методик диагностики. На основе проанализированных показателей с их детализацией можно грамотно выстроить систему защиты от угроз в информационном пространстве.

4 Классификация угроз информационной информации

Классификация всех возможных угроз информационной безопасности автоматизированных систем (АС) может быть проведена по ряду базовых признаков.

1. По природе возникновения.
    - Естественные угрозы — угрозы, вызванные воздействиями на АС и ее компоненты объективных физических процессов или стихийных природных явлений, независящих от человека.
    - Искусственные угрозы — угрозы информационной безопасности АС, вызванные деятельностью человека.
2. По степени преднамеренности проявления.
    - Угрозы случайного действия и/или угрозы, вызванные ошибками или халатностью персонала. Например:
        - проявление ошибок программно-аппаратных средств АС;
        - некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
        - 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.);

- неправомерное включение оборудования или изменение режимов работы устройств и программ;
- неумышленная порча носителей информации;
- пересылка данных по ошибочному адресу абонента (устройства);
- ввод ошибочных данных;
- неумышленное повреждение каналов связи.

- Угрозы преднамеренного действия(например, угрозы действий злоумышленника для хищения информации).

3. По непосредственному источнику угроз.

   - Угрозы, непосредственным источником которых является природная среда(стихийные бедствия, магнитные бури, радиоактивное излучение и т.п.).
   - Угрозы, источником которых является человек:
     - внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);
     - вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;
     - угроза несанкционированного копирования секретных данных пользователем АС;
     - разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).
   - Угрозы, непосредственным источником которых являются санкционированные программно-аппаратные средства:
     - запуск технологических программ, способных при некомпетентном пользовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в си-

стеме (форматирование или реструктуризацию носителей информации, удаление данных и т. п.);
  - возникновение отказа в работе операционной системы.
- Угрозы, непосредственным источником которых являются несанкционированные программно-аппаратные средства:
  - 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);
  - заражение компьютера вирусами с деструктивными функциями.

4. По положению источника угроз.

- Угрозы, источник которых расположен вне контролируемой зоны территории (помещения), на которой находится АС:
  - 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.);
  - 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;
  - дистанционная фото- и видеосъемка.
- Угрозы, источник которых расположен в пределах контролируемой зоны территории (помещения), на которой находится АС:
  - хищение производственных отходов (распечаток, записей, списан-

ных носителей информации и т.п.);
  - отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.д.);
  - применение подслушивающих устройств.
- Угрозы, источник которых имеет доступ к периферийным устройства АС(терминалам).
- Угрозы, источник которых расположен в АС:
  - проектирование архитектуры системы и технологии обработки данных, разработка прикладных программ, которые представляют опасность для работоспособности системы и безопасности информации;
  - некорректное использование ресурсов АС.

5. По степени зависимости от активности АС.
   - Угрозы, которые могут проявляться независимо от активности АС:
     - вскрытие шифров криптозащиты информации;
     - хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и компьютерных систем).
   - Угрозы, которые могут проявляться только в процессе автоматизированной обработки данных(например, угрозы выполнения и распространения программных вирусов).
6. По степени воздействия на АС.
   - Пассивные угрозы, которые при реализации ничего не меняют в структуре и содержании АС (угроза копирования секретных данных).
   - Активные угрозы, которые при воздействии вносят изменения в структуру и содержание АС:
     - внедрение аппаратных спецвложений, программных “закладок” и “вирусов” (“троянских коней” и “жучков”), т.е. таких участков про-

грамм, которые не нужны для выполнения заявленных функций, но позволяют преодолеть систему защиты, скрытно и незаконно осуществить доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;
  - 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.);
  - угроза умышленной модификации информации.

7. По этапам доступа пользователей или программ к ресурсам АС.

   - Угрозы, которые могут проявляться на этапе доступа к ресурсам АС(например, угрозы несанкционированного доступа в АС).
   - Угрозы, которые могут проявляться после разрешения доступа к ресурсам АС(например, угрозы несанкционированного или некорректного использования ресурсов АС).

8. По способу доступа к ресурсам АС.

   - Угрозы, направленные на использование прямого стандартного пути доступа к ресурсам АС:
     - незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, подбором, имитацией интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя (“маскарад”);
     - 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.

- Угрозы, направленные на использование скрытого нестандартного пути доступа к ресурсам АС:
  - вход в систему в обход средств защиты (загрузка посторонней опера ционной системы со сменных магнитных носителей и т.п.);
  - угроза несанкционированного доступа к ресурсам АС путем использования недокументированных возможностей ОС.

9. По текущему месту расположения информации, хранимой и обрабатываемой в АС.

   - Угрозы доступа к информации на внешних запоминающих устройства(например, угроза несанкционированного копирования секретной информации с жесткого диска).
   - Угрозы доступа к информации в оперативной памяти:
     - чтение остаточной информации из оперативной памяти;
     - чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме, используя недостатки мультизадачных АС и систем программирования;
     - угроза доступа к системной области оперативной памяти со сторон прикладных программ.
   - Угрозы доступа к информации, циркулирующей в линиях связи:
     - незаконное подключение к линиям связи с целью работы во время пауз в действиях законного пользователя от его имени с вводом ложных сообщений или модификацией передаваемых сообщений;
     - незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений;
     - перехват всего потока данных с целью дальнейшего анализа не в

реальном масштабе времени.

- Угрозы доступа к информации, отображаемой на терминале или печатаемой на принтере(например, угроза записи отображаемой информации на скрытую видеокамеру). Вне зависимости от конкретных видов угроз или их проблемно-ориентированной классификации АС удовлетворяет потребности эксплуатирующих ее лиц, если обеспечиваются следующие свойства информации систем ее обработки.

Однако самой распространённой классификацией угроз информационной безопасности является классификация по аспекту информационной безопасности, на который направлены угрозы:

- Угрозы конфиденциальности;
- Угрозы целостности;
- Угрозы доступности.

Рассмотрим угрозы доступности.

5 Угрозы доступности

Угроза доступности (отказа служб) возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным — запрашиваемый ресурс никогда не будет получен, или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В этих случаях говорят, что ресурс исчерпан.

Доступность информации — свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда возникает в этом необходимость.

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих ИС. Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники. По некоторым данным, до 65% потерь – следствие непреднамеренных ошибок.

Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе. Самый радикальный способ борьбы с непреднамеренными

ошибками – максимальная автоматизация и строгий контроль.

Другие угрозы доступности классифицируем по компонентам ИС, на которые нацелены угрозы:

- отказ пользователей;
- внутренний отказ информационной системы;
- отказ поддерживающей инфраструктуры.

Обычно применительно к пользователям рассматриваются следующие угрозы:

- нежелание работать с информационной системой;
- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией);
- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Основными источниками внутренних отказов являются:

- отступление от установленных правил эксплуатации;
- выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);
- ошибки при (пере)конфигурировании системы;
- отказы программного и аппаратного обеспечения;
- разрушение данных;
- разрушение или повреждение аппаратуры.

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

- нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
- разрушение или повреждение помещений;
- невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Весьма опасны так называемые “обиженные” сотрудники – нынешние и бывшие. Они стремятся нанести вред организации-“обидчику”, например: - испортить оборудование; - встроить логическую бомбу, которая со временем разрушит программы и/или данные; - удалить данные.

Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.

Опасны, разумеется, стихийные бедствия и события, воспринимаемые как стихийные бедствия, — пожары, наводнения, землетрясения, ураганы. По статистике, на стихийные бедствия (среди которых самый опасный – перебой электропитания) приходится 13% потерь, нанесенных ИС.

6 Выводы

Угрозы информационной безопасности — серьёзная проблема современного мира. Для большего понимания, как с ними бороться, необходимо понимать, откуда и как они появляются. Именно для описания места и причины их появления и существуют различные методы классификации угроз информационной безопасности.

7 Список литературы

1. Краткая характеристика состояния преступности в Российской Федерации за январь-июль 2022 года [Электронный ресурс]. Министерство внутренних дел Российской Федерации, 2022. URL: https://мвд.рф/reports/item/31904956/.
2. Краткая характеристика состояния преступности в Российской Федерации за январь-июль 2023 года [Электронный ресурс]. Министерство внутренних дел Российской Федерации, 2023. URL: https://мвд.рф/reports/item/40874008/.
3. Andress J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. 1st Edition. 2011. 208 с.