Курс: **основы информационной безопасности**

Тема: **Угрозы АС**

Преподаватель: Пятков Антон Геннадьевич

Красноярск

Определения

Уязвимость АС – свойство АС, обуславливающее возможность реализации угроз безопасности обрабатываемой в ней информации

Угроза безопасности – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения конфиденциальности, доступности и/или целостности информации

Источник угрозы ИБ – субъект, являющийся непосредственной причиной возникновения угрозы безопасности информации.

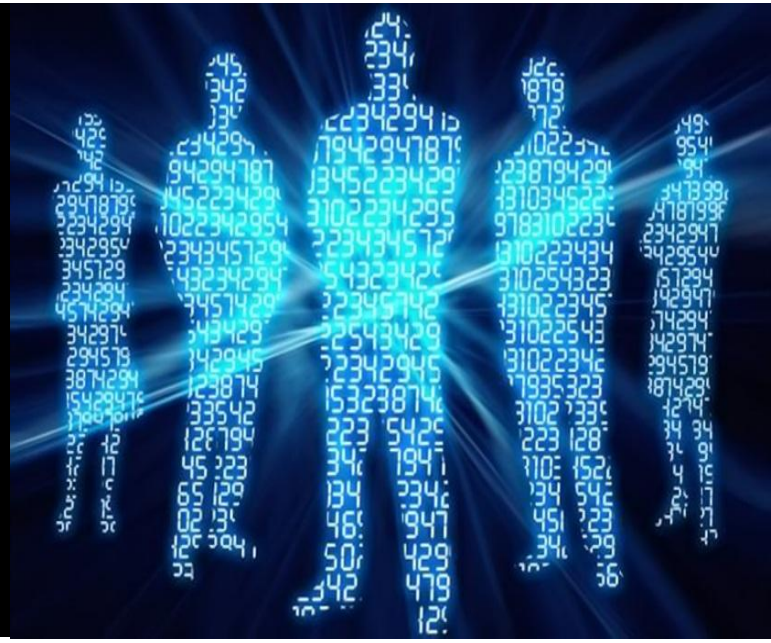
Хакеры

Хакеры - высококвалифицированные IT-специалисты, которые понимают тонкости работы программ, вычислительных систем.

«Компьютерный взломщик» — крэкер, от англ. Crack

Black Hat

White hat



Источники угроз

Основными источниками нарушения безопасности в АС являются:

- аварии и стихийные бедствия (пожар, землетрясение, ураган, наводнение и т.п.);
- сбои и отказы технических средств;
- ошибки проектирования и разработки компонентов АС (программных средств, технологий обработки данных, аппаратных средств и др.);
- ошибки эксплуатации;
- преднамеренные действия нарушителей.

Классификация угроз ИБ АС

1. По природе возникновения: естественные и искусственные

Естественные угрозы - это угрозы, вызванные воздействиями на АС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.

Искусственные угрозы - это угрозы АС, вызванные деятельностью человека.

2. По степени мотивации: непреднамеренные (случайные) и преднамеренные.

Непреднамеренные связаны с разного рода ошибками – в проектировании АС, в программном обеспечении, ошибки персонала при работе с АС и т.п.

Преднамеренные связана с корыстными, идейными и другими целями людей, злоумышленников. Поводом может быть получение материальной выгоды, месть, моральные убеждения и пр.

Классификация угроз ИБ АС

Непреднамеренные (случайные):

- ✔ неумышленные действия, приводящие к нарушению нормального функционирования системы (вплоть до прямого повреждения), либо ее полной остановке;
- ✔ неумышленное отключение оборудования;
- ✔ неумышленная порча носителей информации;
- ✔ использование программного обеспечения, способного при неверном использовании привести к нарушению работоспособности системы (зависанию) или к необратимым изменениям в системе (удаление файлов, форматирование и т.п.);
- ✔ использование программ, которые не нужны для выполнения должностных обязанностей. К ним могут быть отнесены игровые, обучающие и др. программы, использование которых может привести к неумеренному расходу ресурсов системы, в частности, оперативной памяти и процессора;
- ✔ непреднамеренное заражение компьютера вирусами;
- ✔ неосторожные действия, влекущие за собой разглашение информации;
- ✔ ввод ошибочных данных;
- ✔ утрата/передача/разглашение идентификаторов (пароли, ключи, пропуски, ID-карты);
- ✔ построение системы, технологии обработки данных, создание ПО с уязвимостями;
- ✔ несоблюдение политики безопасности или других правил работы с системой;
- ✔ отключение или некорректное использование средств защиты персоналом;
- ✔ пересылка данных по ошибочному адресу абонента (устройства).

Классификация угроз ИБ АС

К основным преднамеренным угрозам можно отнести следующее:

- физическое воздействие на систему или отдельные ее компоненты (устройства, носители, люди), приводящее к выходу из строя, нарушению нормального функционирования;
- отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
- действия по нарушению нормальной работы системы (изменение режимов работы устройств или программ, создание активных радиопомех на частотах работы устройств ,...);
- подкуп, шантаж и другие пути воздействия на персонал или отдельных пользователей, имеющих определенные полномочия;
- применение подслушивающих устройств, дистанционная фото- и видео-съемка и т.п.;
- перехват ПЭМИН;
- перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, данных о системе;
- несанкционированное копирование, хищение носителей информации;
- хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
- чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

Классификация угроз ИБ АС

К основным преднамеренным угрозам можно отнести следующее:

- чтение информации из областей оперативной памяти, используемых ОС (в том числе подсистемой защиты) или другими пользователями;
- 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");
- 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.;
- вскрытие шифров криптозащиты информации;
- внедрение аппаратных , программных "закладок" и "вирусов" ("троянских коней" и "жучков"), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему зашиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;
- незаконное подключение к линиям связи с целью прослушивания, ввода ложных сообщений или модификации 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.

Классификация угроз ИБ АС

3. По положению относительно контролируемой зоны: внутренние и внешние угрозы. В качестве примера внешних угроз может быть перехват данных , передаваемых по сети или утечка через ПЭМИН. К внутренним угрозам можно отнести хищение носителей с конфиденциальной информацией, порчу оборудования, применение различного рода закладок.

Контролируемая зона (КЗ) – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и/или транспортных средств

4. По степени воздействия на АС: пассивные и активные.

Пассивные угрозы – угрозы, не нарушающие состав и нормальную работу АС. Пример – копирование конфиденциальной информации, утечка через технические каналы утечки, подслушивание и т.п.

Активная угроза, соответственно, нарушает нормальное функционирование АС, ее структуру или состав. Например, файловые вирусы, DDOS-атака.

5. По способу реализации: несанкционированный доступ (в том числе случайный) к защищаемой информации, специальное воздействие на информацию, утечка информации через технические каналы утечки.

Несанкционированный доступ (НСД) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

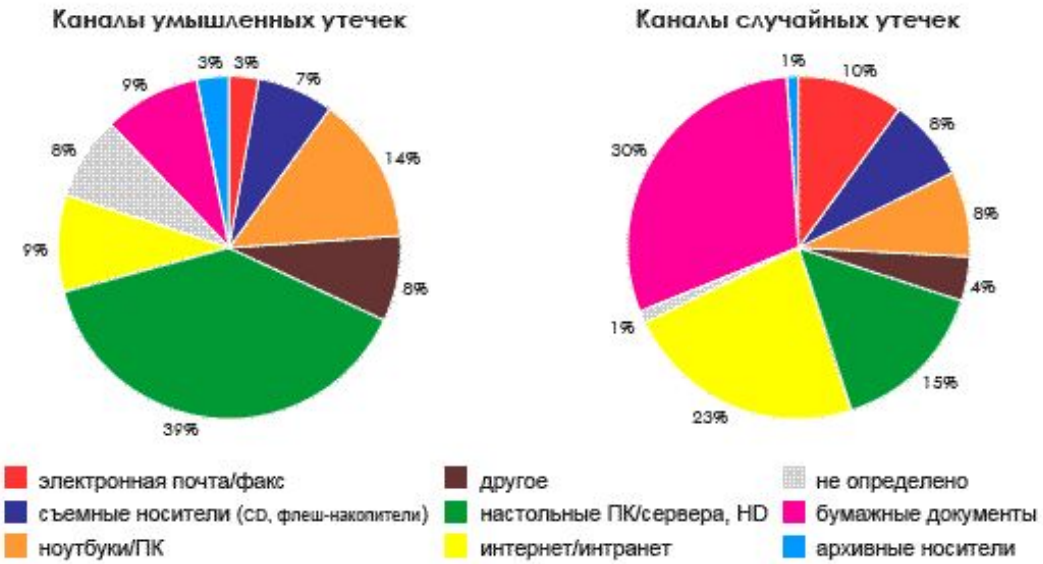
Классификация угроз ИБ АС

6. По виду нарушаемого свойства информации - конфиденциальности, доступности, целостности.

К угрозам доступности можно отнести как искусственные, так и естественные угрозы. Распространены сетевые атаки на доступность информации – DDOS-атаки. Могут быть и естественные: пожар, гроза, наводнение и пр.

Потенциально уязвимыми к нарушению целостности являются не только данные, но и программная среда. Заражение системы вирусом может стать примером реализации угрозы целостности.

К угрозам конфиденциальности можно отнести любые угрозы, связанные с незаконным доступом к информации (перехват передаваемых по сети данных с помощью специальной программы или неправомерный доступ с использованием подобранного пароля, "маскарад" - выполнение действий под видом лица, обладающего полномочиями для доступа к данным).

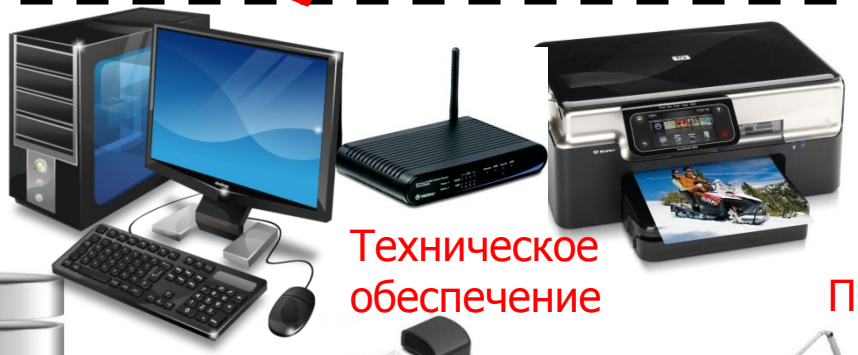


Потенциальные угрозы

Социальная инженерия

Угрозы нарушения КЦД

Персонал



Техническое обеспечение

ПО, алгоритмы

Данные