

Угрозы информации.

Виды угроз безопасности информационных систем

К основным угрозам безопасности информации и нормального функционирования ИС относятся:

- утечка конфиденциальной информации;
- компрометация информации;
- несанкционированное использование информационных ресурсов;
- ошибочное использование информационных ресурсов;
- несанкционированный обмен информацией между абонентами;
- отказ от информации;
- нарушение информационного обслуживания;
- незаконное использование привилегий.

Вредоносные программы классифицируются следующим образом:

- логические бомбы;
- троянский конь;
- компьютерный вирус;
- червь;
- захватчик паролей.

Проблемы защиты информации

Несанкционированный доступ

Несанкционированный доступ к информации — доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

Причины несанкционированного доступа к информации:

- ошибки конфигурации (прав доступа, фаерволов, ограничений на массовость запросов к базам данных);
- слабая защищённость средств авторизации (хищение паролей, смарт-карт, физический доступ к плохо охраняемому оборудованию, доступ к незаблокированным рабочим местам сотрудников в отсутствие сотрудников);
- ошибки в программном обеспечении; - злоупотребление служебными полномочиями (воровство резервных копий, копирование информации на внешние носители при праве доступа к информации);
- прослушивание каналов связи при использовании незащищённых соединений внутри ЛВС;
- использование клавиатурных шпионов, вирусов и троянов на компьютерах сотрудников для имперсонализации.

Приемы несанкционированного доступа к информации:

- За дураком
- За хвост
- Компьютерный абордаж
- Неспешный выбор
- Маскарад
- Мистификация
- Аварийный

Угрозы информационной безопасности – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. **Атакой** называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, - **злоумышленником**. Потенциальные злоумышленники называются *источниками угрозы*.

Угроза является следствием наличия уязвимых мест или уязвимостей в информационной системе. Уязвимости могут возникать по разным причинам, например, в результате непреднамеренных ошибок программистов при написании программ.

Угрозы можно классифицировать по нескольким критериям:

- по **свойствам информации** (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;
- по **компонентам информационных систем**, на которые угрозы нацелены (данные, программы, аппаратура, *поддерживающая инфраструктура*);
- по **способу осуществления** (случайные/преднамеренные, действия природного/техногенного характера);
- по **расположению источника угроз** (внутри/вне рассматриваемой ИС).

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется *комплексный подход*. Выделяют следующие уровни защиты информации:

- **законодательный** – законы, нормативные акты и прочие документы РФ и международного сообщества;
- **административный** – комплекс мер, предпринимаемых локально руководством организации;
- **процедурный уровень** – меры безопасности, реализуемые людьми;
- **программно-технический уровень** – непосредственно средства защиты информации.

Законодательный уровень является основой для построения системы защиты информации, так как дает базовые понятия *предметной области* и определяет меру наказания для потенциальных злоумышленников. Этот уровень играет координирующую и направляющую роли и помогает поддерживать в обществе негативное (и карательное) *отношение* к людям, нарушающим информационную *безопасность*.

Угрозы можно классифицировать по нескольким критериям:

- по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

Наиболее распространенные угрозы доступности

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

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 (таковы обычно ошибки администрирования). По некоторым данным, до 65% потерь - следствие непреднамеренных ошибок.

Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе.

Очевидно, 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 (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);
- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);
- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.)

Основными источниками внутренних отказов являются:

- отступление (случайное или умышленное) 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. Как правило, они стремятся нанести вред организации-"обидчику", например:

- испортить оборудование;
- встроить логическую бомбу, которая со временем разрушит программы и/или данные;
- удалить данные.

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.