Информатика и информационно-коммуникационные технологии

Сафарьян Ольга Александровна

Лекция 8

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Угрозы информационной безопасности
2. Методы и средства защиты информации
3. Правовые основы информационной безопасности
4. Компьютерные вирусы и вредоносные программы
5. Методы защиты от вирусов
6. Криптографические механизмы защиты информации

Угрозы информационной безопасности

- **Конфиденциальность** – свойство информации быть доступной только ограниченному кругу субъектов доступа.
- **Целостность** – свойство информации сохранять свою структуру и содержание в процессе хранения, использования и передачи.
- **Доступ** – возможность субъекта осуществлять определенные действия с информацией. При выполнении правил разграничения доступа – санкционированный (иначе – несанкционированный).
- Под **угрозой информационной безопасности** понимается действие или событие, которое может привести к разрушению, искажению или несанкционированному использованию информационных ресурсов, включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства. Деляться на **случайные** или непреднамеренные, и **умышленные**.

- **Пассивные** угрозы, как правило, направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на функционирование системы.
- **Активные** угрозы имеют цель: нарушить нормальный процесс функционирования системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы.

К основным угрозам безопасности информации относят:

- раскрытие конфиденциальной информации;
- компрометация информации;
- несанкционированное использование информационных ресурсов;
- ошибочное использование информационных ресурсов;
- несанкционированный обмен информацией;
- отказ от информации;
- отказ в обслуживании.

- **Компрометация информации**, как правило, реализуется посредством внесения несанкционированных изменений в базы данных, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений.
- **Несанкционированное использование** информационных ресурсов, с одной стороны, является средством раскрытия или компрометации информации, а с другой — имеет самостоятельное значение, поскольку, даже не касаясь пользовательской или системной информации, может нанести определенный ущерб абонентам и администрации.
- **Ошибочное использование** информационных ресурсов, будучи санкционированным, тем не менее, может привести к разрушению, раскрытию или компрометации указанных ресурсов.
- **Несанкционированный обмен** информацией между абонентами может привести к получению одним из них сведений, доступ к которым ему запрещен, что по своим последствиям равносильно раскрытию содержания банковской информации.
- **Отказ от информации** состоит в непризнании получателем или отправителем этой информации фактов ее получения или отправки.
- **Отказ в обслуживании** представляет собой весьма существенную и распространенную угрозу, источником которой является сама система и применяемые в ней технологии.

Методы и средства защиты информации

Создание базовой системы защиты информации основывается на следующих принципах:

- **Комплексный подход** к построению системы защиты при ведущей роли организационных мероприятий, означающий оптимальное сочетание программных аппаратных средств и организационных мер защиты и подтвержденный практикой создания отечественных и зарубежных систем защиты.
- **Разделение** и **минимизация** полномочий по доступу к обрабатываемой информации и процедурам обработки, т.е. предоставление пользователям минимума строго определенных полномочий, достаточных для успешного выполнения ими своих служебных обязанностей, с точки зрения автоматизированной обработки доступной им конфиденциальной информации.
- **Полнота контроля** и регистрации попыток несанкционированного доступа, т.е. необходимость точного установления идентичности каждого пользователя и протоколирования его действий для проведения возможного расследования, а также невозможность совершения любой операции обработки информации в системе без ее предварительной регистрации..

- **Обеспечение надежности** системы защиты, т.е. невозможность снижения уровня надежности при возникновении в системе сбоев, отказов, преднамеренных действий нарушителя или непреднамеренных ошибок пользователей и обслуживающего персонала.
- **Обеспечение контроля** за функционированием системы защиты, т.е. создание средств и методов контроля работоспособности механизмов защиты.
- **«Прозрачность»** системы защиты информации для общего, прикладного программного обеспечения и пользователей.
- **Экономическая целесообразность** использования системы защиты, выражающаяся в том, что стоимость разработки и эксплуатации систем защиты информации должна быть меньше стоимости возможного ущерба, наносимого объекту в случае его разработки и эксплуатации без системы защиты информации.
- Следует отметить, что какими бы совершенными не были программно-технические средства защиты информации от несанкционированного доступа, без надлежащей организационной поддержки и точного выполнения предусмотренных проектной документацией процедур проблему обеспечения безопасности информации в должной мере не решить.

Рассмотрим методы и средства обеспечения безопасности информации, составляющие основу механизмов защиты.

- **Препятствие** – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т. д.).
- **Управление доступом** – метод защиты информации регулированием использования всех ресурсов компьютерной информационной системы (элементов баз данных, программных и технических средств).

Управление доступом включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);
- аутентификация (опознание, установление подлинности) объекта или субъекта по предъявленному им идентификатору;
- проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);
- разрешение и создание условий работы в пределах установленного регламента;
- регистрацию (протоколирование) обращений к защищаемым ресурсам;
- реагирование (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.

- **Маскировка** – метод защиты информации путем ее криптографического закрытия. Этот метод защиты широко применяется за рубежом как при обработке, так и при хранении информации, в том числе на дискетах. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.
- **Регламентация** – метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.
- **Принуждение** – такой метод защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.
- **Побуждение** – такой метод защиты, который побуждает пользователя и персонал системы не разрушать установленные порядки за счет соблюдения сложившихся моральных и этических норм (как регламентированных, так и неписаных).
- Рассмотренные методы обеспечения безопасности реализуются на практике за счет применения различных средств защиты, таких как технические, программные, организационные, законодательные и морально-этические.

Основные средства защиты делятся на **формальные** (выполняющие защитные функции строго по заранее предусмотренной процедуре без непосредственного участия человека) и **неформальные** (определяются целенаправленной деятельностью человека либо регламентируют эту деятельность).

К формальным средствам относятся следующие:

- – *Технические* средства реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на физические и аппаратные.
- – *Физические* средства реализуются в виде автономных устройств и систем. Например, замки на дверях, где размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации.
- – Под *аппаратными* техническими средствами принято понимать устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу.
- – *Программные* средства представляют из себя программное обеспечение, специально предназначенное для выполнения функций защиты информации.

Неформальные средства:

- – *Организационные* средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации вычислительной техники, аппаратуры телекоммуникаций для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы аппаратуры на всех этапах их жизненного цикла (строительство помещений, проектирование компьютерной информационной системы банковской деятельности, монтаж и наладка оборудования, испытания, эксплуатация).
- – *Законодательные* средства защиты определяются законодательными актами, которыми регламентируются правила пользования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.
- – *Морально-этические* средства защиты реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи в обществе. Эти нормы большей частью не являются обязательными как законодательные меры, однако несоблюдение их ведет обычно к потере авторитета и престижа человека.

Правовые основы информационной безопасности

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

- свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- установление ограничений доступа к информации только федеральными законами;
- открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
- обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- достоверность информации и своевременность ее предоставления;
- неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных

К сфере информационной безопасности относится также Федеральный закон «Об электронной подписи», регулирующий отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий.

Неквалифицированной электронной подписью является электронная подпись, которая:

- 1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- 2) позволяет определить лицо, подписавшее электронный документ;
- 3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- 4) создается с использованием средств электронной подписи.

Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим дополнительным признакам:

- 1) ключ проверки электронной подписи указан в квалифицированном сертификате;
- 2) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным законом.

Нарушение законов влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Компьютерные вирусы и вредоносные программы

Вирус – программа, которая может приписывать себя к другим программам, т.е. «заражать» их, а также выполнять различные нежелательные действия в компьютере. Основным свойством компьютерного вируса является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и(или) файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

Вирусы можно разделить на классы по следующим основным признакам:

- *среда обитания (заражаемые объекты);*
- *тип операционной системы, платформы;*
- *особенности алгоритма работы; деструктивные возможности и вредоносная функциональность.*

По среде обитания можно выделить следующие типы вирусов: файловые;

загрузочные; макро-; сетевые.

- Файловые вирусы различными способами внедряются в выполняемые файлы (первоначально – наиболее распространенный тип вирусов).
- Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера Master Boot Record (MBR), либо меняют указатель на активный boot-сектор.
- Макровирусы являются программами на макроязыках, встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т.д.).
- Сетевые вирусы, их также называют сетевыми червями (worms), используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

По *особенностям алгоритма работы* вирусов выделяются следующие разновидности:

- стелс-вирусы (англ. *stealth virus* – вирус-невидимка);
- полиморфные вирусы (англ. *polymorphic viruses*. от греч. *πολυ* – много, *μορφή* – форма, вид);
- использование нестандартных приемов.

Метасимволы или маски. Не всякая поисковая машина может поддерживать поиск строк с использованием метасимволов – «*» и «?», которые обычно используются в значении «любое количество любых символов» и «произвольный (любой) одиночный символ» соответственно. Тем не менее, эти операторы нередко бывают зарезервированы для подобного использования в будущем.

Знание языка запросов и умение его использовать даёт возможность сделать поиск более эффективным и результативным, что немаловажно для успешного освоения выбранной профессии в вузе и дальнейшей профессиональной деятельности.

К вредоносным и нежелательным, помимо вирусов, примыкают следующие программы: конструкторы вирусов, полиморфик-генераторы; «троянские кони», к которым относятся всевозможные кейлоггеры, «ворующие» пароли и прочую конфиденциальную информацию; сканеры, снифферы (прослушиватели сети); люки – утилиты скрытого администрирования удаленных компьютеров (backdoor); логические бомбы; руткиты (англ. *rootkit* – набор инструментов root'а, то есть суперпользователя, учётная запись которого в UNIX по умолчанию именуется root – корень), предназначенные для «заметания следов» вторжения злоумышленника, маскировки вредоносной программы, а также самого присутствия руткита в системе путём сокрытия файлов и процессов; программы взлома (crack) защитных функций лицензионного ПО и другие.

Методы защиты от вирусов

Существующие методы защиты от вирусов и прочих вредоносных программ можно разделить на следующие группы:

- профилактические меры;
- специализированные программы;
- программно-аппаратные средства.

Охарактеризуем антивирусы:

Детекторы только ищут в памяти и в файлах характерные коды (сигнатуры) вирусов и выдают соответствующее сообщение при их обнаружении.

Доктора (фаги, полифаги) не только детектируют, но и удаляют из зараженных объектов коды вирусов.

Сканеры запускаются пользователем и позволяют задать область (диск, папку, файлы) и параметры сканирования.

Мониторы являются резидентными (постоянно находящимися в оперативной памяти и выполняющими проверку «на лету») программами. Обычно они помещаются в оперативную память после загрузки операционной системы, находятся в памяти во время всего сеанса работы и отслеживают операции с дисками и памятью.

Классические антивирусные продукты обнаруживают фиксированный набор известных вирусов, сигнатуры которых содержатся в их вирусных базах. Из-за огромного постоянно растущего количества новых вирусов и их модификаций сигнатурные методы обнаружения уже не могут обеспечить эффективную защиту

Криптографические механизмы защиты информации

Криптология – наука, состоящая из двух ветвей: криптографии и криптоанализа.
Криптография – наука о методах преобразования (шифрования) информации с целью сокрытия и защиты ее от незаконных пользователей.
Криптоанализ – наука (и практика ее применения) о методах и способах вскрытия шифров.
Ключ – сменный элемент шифра, который применен для шифрования конкретного сообщения.
По характеру использования ключа известные криптосистемы можно разделить на симметричные (одноключевые, с секретным ключом) и асимметричные (с открытым ключом).
Симметричные системы основаны на использовании одного и того же секретного ключа для шифрования и дешифрования.
Асимметричные характеризуются тем, что для шифрования используется один ключ, являющийся общедоступным.

Основ информационной безопасности:

- **Автоматизация (без которой невозможно развитие современных информационных систем) приводит к росту угроз несанкционированного доступа к информации и, как следствие, к необходимости постоянной поддержки и развития систем защиты.**
- **Защита информации является не разовым мероприятием и даже не совокупностью мероприятий, а непрерывным процессом, который должен протекать на всех этапах жизненного цикла информационной системы.**
- **Создание эффективных средств защиты может быть осуществлено только высококвалифицированными специалистами.**
- **Анализ, оценку, проектирование и сертификацию системы защиты информации необходимо проводить независимыми организациями, имеющими государственную лицензию на проведение указанных работ.**
- **Комплексное решение проблем защиты информации в компьютерных системах требует вложения значительных средств.**