Группа Ф-21. Дата 22.05.2020

Преподаватель: Тимофеева С.Н.

Учебная дисциплина «Информационные технологии в профессиональной деятельности»

Специальность 32.02.06 Финансы

Задание 15. Изучение темы **Обеспечение информационной безопасности** по плану. Составьте по данным вопросам опорный конспект и словарь основных терминов. Укажите информационные ресурсы при составлении конспекта.

Задания для самостоятельной работы студентов

Составление и проработка конспекта занятия, работа с информационными порталами, выполнение домашних заданий.

Выполненные задания отправлять на e-mail: timsnikol@mail.ru

Тема 3.2: Обеспечение информационной безопасности

Цели: познакомиться с понятием информационной безопасности

- рассмотреть различные угрозы информационной безопасности

Основные понятия и термины по теме: информационная и компьютерная безопасность компьютерные вирусы, целостность информации, несанкционированный доступ, идентификация, аутентификация, защита информации.

План изучения темы

1. Основные угрозы и методы обеспечения информационной безопасности.
2. Классификация средств защиты.
3. Виды компьютерных вирусов. Методы распространения компьютерных вирусов и профилактика от заражения. Организация защиты от компьютерных вирусов.
4. Организация безопасной работы с компьютерной техникой.

Краткое изложение теоретических вопросов

Информационная безопасность – это состояние защищенности субъектов РФ в информационной сфере, отражающих совокупность сбалансированных интересов личности, общества и государства.

Официальная политика служат основой:

- Для формирования государственной политики в области обеспечения информационной безопасности РФ.

- Подготовки предложений по совершенствованию правового, методического , научно-технического и организационного обеспечения информационной безопасности РФ.
- Разработки целевых программ обеспечения информационной безопасности РФ

Под **безопасностью информации** понимается защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Под **доступностью информации** понимается свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

Под **целостностью информации** понимается свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

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;
- нарушение информационного обслуживания;
- незаконное использование привилегий.

Утечка конфиденциальной информации – это бесконтрольный выход конфиденциальной информации за пределы ИС или круга лиц, которым она была доверена по службе или стала известна в процессе работы.

Несанкционированный доступ – это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям

Вирус – программа, которая может заражать другие программы путем включения в них модифицированной копии, которая в свою очередь сохраняет способность к дальнейшему размножению

Считается, что вирус характеризуется двумя основными особенностями:

1) способностью к саморазмножению (созданию собственных копий);

2) наличием механизма, обеспечивающего внедрение создаваемых копий в исполняемые объекты вычислительной системы.

Идентификация – это присвоение пользователю уникального обозначения для проверки его соответствия.

Аутентификация – установление подлинности пользователя для проверки его соответствия.

Защита информации - комплекс мероприятий, направленных на обеспечение целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных.

На сегодняшний день сформулировано два базовых принципа по защите информации:

· целостность данных - защита от сбоев, ведущих к потере информации, а также защита от неавторизованного создания или уничтожения данных;

· конфиденциальность информации.

Виды, методы и средства защиты информации

В условиях использования АИТ под **безопасностью** понимается состояние защищенности ИС от внутренних и внешних угроз.

Политика безопасности – это набор законов, правил и практического опыта, на основе которых строится управление, защита и распределение конфиденциальной информации

Методы и средства обеспечения безопасности информации в АИС:

К основным методам защиты информации относятся:

1. повышение достоверности информации;
2. криптографическое преобразование информации;
3. контроль и учет доступа к внутреннему монтажу аппаратуры, линиям связи и технологическим органам управления;
4. ограничение доступа;
5. разграничение и контроль доступа к информации;
6. разделение доступа (привилегий);
7. идентификация и аутентификация пользователей, технических средств, носителей информации и документов.

Препятствие – метод физического преграждения пути злоумышленнику к защищаемой информации (к аппаратуре, носителям информации и т.д.).

Управление доступом – методы защиты информации регулированием использования всех ресурсов ИС и ИТ. Эти методы должны противостоять всем

возможным путям несанкционированного доступа к информации. Кроме того, управление доступом включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);
- аутентификацию для опознания, установления подлинности пользователя 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 и т.п.) при попытках несанкционированных действий.

Шифрование – криптографическое закрытие информации. Эти методы защиты все шире применяются как при обработке, так и при хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.

Кодирование информации – это преобразование информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и ввода-вывода.

Противодействие атакам вредоносных программ – комплекс разнообразных мер организационного характера и по использованию антивирусных программ. Цели принимаемых мер: уменьшение вероятности инфицирования АИС; выявление фактов заражения системы; уменьшение последствий информационных инфекций; локализация или уничтожение вирусов; восстановление информации в ИС.

Из средств ПО системы защиты выделим еще программные средства, реализующие механизмы шифрования (криптографии). **Криптография** – это наука об обеспечении секретности и/или аутентичности (подлинности) передаваемых сообщений.

Организационные (административные) средства осуществляют своим комплексом регламентацию производственной деятельности в ИС и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становится невозможным или существенно затрудняется за счет проведения организационных мероприятий. Комплекс этих мер реализуется группой информационной безопасности, но должен находиться под контролем руководителя организации.

Законодательные (правовые) средства защиты определяются законодательными актами страны, которыми регламентируются правила пользования, обработки и передачи

информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Морально-этические средства защиты включают всевозможные нормы поведения, которые традиционно сложились ранее, складываются по мере распространения ИС и ИТ в стране и в мире.

Вся совокупность технических средств подразделяется на аппаратные и физические.

Аппаратные (технические) средства – устройства, встраиваемые непосредственно в вычислительную технику, или устройства, которые сопрягаются с ней по стандартному интерфейсу.

Физические средства включают различные инженерные устройства и сооружения, препятствующие физическому проникновению злоумышленников на объекты защиты и осуществляющие защиту персонала (личные средства безопасности), материальных средств и финансов, информации от противоправных действий. Примеры физических средств: замки на дверях, решетки на окнах, средства электронной охранной сигнализации и т.п.

Программные средства – специализированные программы и программные комплексы, предназначенные для защиты информации в ИС.

Вредоносные программы классифицируются следующим образом.

Классификация вирусов:

1) **по деструктивным возможностям:**
   - ✓ безвредные – никак не влияющие на работу компьютера кроме уменьшения свободной памяти на диске в результате своего распространения;
   - ✓ неопасные – влияние ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами;
   - ✓ опасные – могут привести к серьезным сбоям в работе компьютера;
   - ✓ очень опасные – в алгоритм работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти;
2) **по среде обитания:**
   - ✓ файловые – вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы;
   - ✓ загрузочные – вирусы записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера;

- ✓ макровирусы – вирусы заражают файлы-документы и электронные таблицы популярных редакторов;
- ✓ сетевые – вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты;

3) **по особенностям алгоритма работы:**

«Логические бомбы», как вытекает из названия, используются для искажения или уничтожения информации; реже с их помощью совершаются кража или мошенничество. Реальный пример «логической бомбы»: программист, предвидя свое увольнение, вносит в программу расчета заработной платы определенные изменения, работа которых начинается, если его фамилия исчезнет из набора данных о персонале фирмы.

«Троянский конь» - программа, выполняющая в дополнение к основным, т.е. запроектированным и документированным, действиям действия дополнительные, но не описанные в документации. «Троянский конь» представляет собой дополнительный блок команд, тем или иным образом вставленный в исходную безвредную программу, которая затем передается (дарится, продается, подменяется) пользователям ИС. Этот блок команд может срабатывать при наступлении некоторого условия (даты, времени, по команде извне и т.д. Наиболее опасные действия «троянский конь» может выполнять, если запустивший его пользователь обладает расширенным набором привилегий. В таком случае злоумышленник, составивший и внедривший «троянского коня», и сам этими привилегиями не обладающий, может выполнять несанкционированные привилегированные функции чужими руками.

«Червь» - программа, распространяющаяся через сеть и не оставляющая своей копии на магнитном носителе. «Червь» использует механизмы поддержки сети для определения узла, который может быть заражен. Затем с помощью тех же механизмов передает свое тело или его часть на этот узел и либо активизируется, либо ждет для этого подходящих условий. Наилучший способ защиты от «червя» – принятие мер предосторожности против несанкционированного доступа к сети.

Особенности защиты информации в ПЭВМ

Особенностями ПЭВМ с точки зрения защиты информации являются:

малые габариты и вес, что делает их легко переносимыми;

наличие встроенного внутреннего запоминающего устройства большого объема, сохраняющего записанные данные после выключения питания;

наличие сменного запоминающего устройства большого объема и малых габаритов;

наличие устройств сопряжения с каналами связи;

оснащенность программным обеспечением с широкими функциональными возможностями.

Основная цель защиты информации в ПЭВМ заключается в обеспечение ее физической целостности и предупреждении несанкционированного доступа к ней.

В самом общем виде данная цель достигается путем ограничения доступа посторонних лиц в помещения, где находятся ПЭВМ, а также хранением сменных запоминающих устройств и самих ПЭВМ с важной информацией в нерабочее время в опечатанном сейфе.

Наряду с этим для предупреждения несанкционированного доступа к информации используются следующие методы:

- опознавание (аутентификация) пользователей и используемых компонентов обработки информации;
- разграничение доступа к элементам защищаемой информации;
- регистрация всех обращений к защищаемой информации;
- криптографическое закрытие защищаемой информации в процессе ее непосредственной обработки.

Разграничение доступа к элементам защищаемой информации заключается в том, чтобы каждому зарегистрированному пользователю предоставить возможности беспрепятственного доступа к информации в пределах его полномочий и исключить возможности превышения своих полномочий

Регистрация всех обращений к защищаемой информации осуществляется с помощью устройств, которые контролируют использование защищаемой информации, выявляют попытки несанкционированного доступа к ней, накапливают статистические данные о функционировании системы защиты.

Программы архивации - это программы, позволяющие уменьшить размер файла для сохранения его на съемном носителе, передачи по сети, защите информации, а также для экономии места на диске. Файлы можно скопировать в архив, т.е. создать архив и не

удалять исходные файлы с диска, а можно переместить в архив, т.е. создать архив и удалить исходные файлы с диска.

Файлы, находящиеся в архиве, можно извлечь из архива (говорят также разархивировать или распаковать), т.е. восстановить их на диске в том виде, который они имели до архивации.

Вопросы для самоконтроля

1. Понятие компьютерного вируса, защиты информации и информационной безопасности. Принципы и способы защиты информации в информационных системах.
2. Характеристика угроз безопасности информации и их источников. Методы обеспечения информационной безопасности.
3. Принципы защиты информации от несанкционированного доступа.
4. Правовое обеспечение применения информационных технологий и защиты информации

Задания для самостоятельного выполнения

1. Назовите основные угрозы и методы обеспечения информационной безопасности
2. Какие виды умышленных угроз безопасности информации вам известны?
3. Классифицируйте информационные угрозы безопасности информации
4. Виды, методы и средства защиты информации
5. Особенности защиты информации в ПЭВМ

Д/задание

Подготовить доклады и презентации на тему:

«Характеристика угроз безопасности информации и их источников»;

Создание презентации «Антивирусная защита информации».

Информационный ресурс

1. https://xn----7sbbfb7a7aej.xn--p1ai/informatika_11/informatika_materialy_zanytii_11_06.html