Лекция 8

Технологии безопасности и защиты информации. Эргономика

План лекции:

- 1. Безопасность программно-технических средств и информационных ресурсов. Защита данных
- 2. Криптографическая защита информации
- 3. Электронная подпись
- 4. Технические возможности и мероприятия по обеспечению сохранности людей, зданий, помещений, программно-технических средств и информации
- 5. Охрана объектов с целью ограничения свободного доступа, смарткарты и др.

1. Безопасность программно-технических средств и информационных ресурсов. Защита данных

- Практически вся современная информация готовится или может быть достаточно легко преобразована в машиночитаемую форму. Характерной особенностью такой информации является возможность посторонних лиц легко и незаметно исказить, скопировать или уничтожить её. Это обстоятельство вызывает насущную потребность организации безопасного функционирования данных в любых информационных системах (компьютерных сетях). Такие мероприятия называют защитой информации или информационной безопасностью. Противоправные действия с информацией не только затрагивают интересы государства, общества и личности, но оказывают негативные, а порой трагические и катастрофические воздействия на здания, помещения, личную безопасность обслуживающего персонала и пользователей информации. Подобные воздействия происходят по причине стихийных бедствий, техногенных катастроф и террористических актов.

- Общеизвестно, что «безопасность» – отсутствие опасности; состояние деятельности, при которой с определённой вероятностью исключено причинение ущерба здоровью человека, зданиям, помещениям и материально-техническим средствам в них. Терминологически в Толковом словаре «безопасность» трактуется как состояние субъекта, при котором отсутствует угроза нанесения ему какого-либо ущерба.

- Под безопасностью информации (Information security) или информационной безопасностью понимают защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам и пользователям информации и поддерживающей её структуре.
- Защищённой считают информацию, не претерпевшую несанкционированных изменений в процессе передачи, хранения и сохранения, не изменившую такие свойства, как достоверность, полнота и целостность данных.
- Под терминами «защита информации» и «информационная безопасность» подразумевается совокупность методов, средств и мероприятий, направленных на исключение искажений, уничтожения и не- санкционированного использования накапливаемых, обрабатываемых и хранимых данных.

- В законе «Об информации, информатизации и защите информации» (ст. 20) определено, что целями защиты информации являются: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокировке информации

- Широкий спектр средств и методов защиты информации обычно делят на две группы: организационные и технические. Под организационными подразумеваются законодательные, административные и физические, а под техническими – аппаратные, программные и криптографические.

- Организационные методы защиты информации базируются на: 1) определении ответственного за информационную безопасность, в функции которого входит управление рисками, координация и контроль деятельности в области информационной безопасности и стратегическое планирование в организации;
- 2) обеспечении надёжной и экономичной защиты (средства и методы защиты, программно-технические средства, постоянное администрирование и т.п.) ИР, связанных с ними людей и помещений (зданий).

- С целью организации защиты объектов используют системы охраны и безопасности объектов – совокупность взаимодействующих радиоэлектронных приборов, устройств и электрооборудования, средств технической укреплённости и инженерной защиты, специально подготовленного персонала, а также транспорта, выполняющих названную функцию

- При рассмотрении проблем, связанных с обеспечением безопасности, используют понятие «несанкционированный доступ» – неправомочное обращение к информационным ресурсам с целью их непредусмотренного использования (чтения, модификации), а также порчи или уничтожения. Данное понятие также связано с непредсказуемым распространением разного рода компьютерных вирусов (в том числе «спама»).
- В свою очередь «санкционированный доступ» (англ. – «authorized access») – доступ к программам и данным пользователей, имеющих право выполнять определенные действия (чтение, копирование, изменение и др.), а также полномочия и права пользователей на использование ресурсов и услуг, определённых администратором вычислительной системы.

- Аутентификация – установление подлинности информации на основе подлинности её внутренней структуры независимо от её источника.
- Идентификация – отожествление предметов или лиц по их характеристикам или путём опознавания по предметам или документам и определение полномочий, связанных с их доступом в помещения, к документам и т.д.

- Программные средства защиты – самый распространенный метод защиты информации в компьютерах и информационных сетях. Наиболее часто они применяются в случаях затруднения использования других методов и средств. Программные средства защиты информации представляют комплекс алгоритмов и программ специального назначения и общего обеспечения функционирования компьютеров и информационных сетей, на- целенных на: контроль и разграничение доступа к информации, исключение несанкционированных действий с ней, управление охранными устройствами и т.п. Они обладают универсальностью, простотой реализации, гибкостью, адаптивностью, возможностью настройки системы и др.

2. Криптографическая защита информации

- Одним из наиболее практикуемых современных способов защиты информации, является её кодирование (шифрование). Оно не спасает от физических воздействий, но в остальных случаях служит весьма надёжным средством. Кодом называют правила составления различных сигналов, изображений и алфавитов

- Код характеризуется: длиной – числом позиций (знаков, используемых при кодировании) и структурой – порядком расположения символов, используемых для обозначения классификационного признака. Средством кодирования служит таблица соответствия. Примером такой таблицы для перевода алфавитно-цифровой информации в компьютерные коды является кодовая таблица ASCII

- Для предотвращения несанкционированного использования данных на машинных носителях применяются разные системы кодирования (шифрования) информации. Сокрытия смысла (содержания) информации обеспечивается, как правило, с помощью алфавитно-цифровых шрифтов и цифровых кодов соответственно. Первый стандарт шифрования опубликован в 1977 году в США.

- Всё большую популярность приобретают криптографические методы защиты информации, представляющие комплекс (совокупность) алгоритмов и процедур шифрования и кодирования информации для обеспечения преобразования смыслового содержания передаваемой в информационных сетях данных, то есть подразумевают создание специальных секретных ключей пользователей.

- Криптография – тайнопись, система изменения информации с целью её защиты от несанкционированных воздействий, а также обеспечения достоверности передаваемых данных. Общие методы криптографии существуют достаточно давно, и она, по праву, считается мощным средством обеспечения конфиденциальности и контроля целостности информации. Как утверждают многие специалисты, альтернативы методам криптографии ныне нет.
- Основу криптографии составляют алгоритмы преобразования данных, использующие методы перестановки и подстановки (замены), алгебру матриц (аналитические преобразования) и др. Стойкость крипто- алгоритма зависит от сложности методов преобразования.

3. Электронная подпись

- Одной из важных проблем информационной безопасности является организация защиты электронных данных и электронных документов. Для кодирования ЭИР, с целью удовлетворения требованиям обеспечения безопасности данных от несанкционированных воздействий на них, используется электронная цифровая подпись (ЭЦП).

- Первый отечественный стандарт ЭЦП появился в 1994 году – ГОСТ Р34.10-94 «Информационная технология. Криптографическая за щита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».
- Новая редакция этого закона принята 12 сентября 2001 года постановлением Госстандарта России №380-ст.– ГОСТ Р 34.10-2001. Анало- гичный стандарт ЭЦП в США принят в 1994 году (FIPS 186).
- В законе об ЭЦП электронный документ определяется как «…документ, в котором информация представлена в электронно-цифровой форме»

- Цифровая подпись для сообщения является последовательностью символов, зависящей от самого сообщения и от некоторого секретного, известного только подписывающему субъекту, ключа.
- Она должна легко проверяться и позволять решать три следующие задачи:
- ● осуществлять аутентификацию источника сообщения,
- ● устанавливать целостность сообщения,
- ● обеспечивать невозможность отказа от факта подписи конкретного сообщения.

4. Технические возможности и мероприятия по обеспечению сохранности людей, зданий, помещений, программно-технических средств и информации

- Организационные мероприятия предполагают объединение всех составляющих (компонент) безопасности. Согласно многочисленным статистическим данным во всём мире основную угрозу ИР организации представляют её сотрудники, оказывающиеся психически неуравновешенными, обиженными или неудовлетворенными характером их работы, заработной платой, взаимоотношениями с коллегами и руководителями.

- Физические в большей степени примыкают к организационным мероприятиям, нацеленным на реализацию названной цели. Они заключаются в применении человеческих ресурсов, отдельных технических средств и устройств, позволяющих обеспечивать защиту от проникновения злоумышленников на объект, несанкционированного использования, порчи или уничтожения ими материальных и людских ресурсов. Такими человеческими ресурсами являются лица ведомственной или вневедомственной охраны и вахтеры, а также отдельные, назначаемые руководством организации, сотрудники. Они ограничивают, в том числе с помощью соответствующих технических устройств, доступ на объекты нежелательных лиц.
- В качестве технических средств используются решётки на окна, ограждения, металлические двери, турникеты и др. Программно- технические средства включают различные системы ограничения доступа на объект, сигнализации и видеонаблюдения.

- Технические мероприятия включают в себя элементы физических мероприятий. Они базируются на применении следующих технических средств и систем:
- ● охранной и пожарной сигнализации;
- ● контроля и управления доступом;
- ● видеонаблюдения и защиты периметров объектов;
- ● защиты информации;
- ● контроля состояния окружающей среды и технологического оборудования, систем безопасности, перемещения людей, транспорта и грузов;
- ● учёта рабочего времени персонала и времени присутствия на объектах различных посетителей.

- Для комплексного обеспечения безопасности объекты оборудуются системами связи, диспетчеризации, оповещения, контроля и управления доступом; охранными, пожарными, телевизионными и инженерными устройствами и системами; охранной, пожарной сигнализацией, противопожарной автоматикой и др.

- Социально-психологические мероприятия также относятся к организационным. Они включают регулярное проведение организационных мероприятий по недопущению отрицательных воздействий и явлений, по созданию работникам комфортных условий и нормального психологического климата. С этой целью в штат некоторых организаций входит психолог. Успешному обеспечению безопасности способствуют заблаговременные мероприятия по выявлению и идентификации возможных угроз (опознание и предвидение, оценка, уменьшение вредного влияния их на человека и среду его обитания).

- Охрана зданий и помещений предполагает решение следующих задач:
- 1) создание физической защиты внутри и снаружи зданий и помещений (решётки на окнах, металлические двери, турникеты и другие устройства, в том числе технические и (или) программно-технические средства ограничения несанкционированного посещения территории и отдельных помещений);
- 2) организация службы охраны, в которую могут входить: вахтеры, работники ведомственной или вневедомственной охраны, собственной службы безопасности и сотрудники организации, добровольно или в административном порядке участвующие в её охране с целью ограничения доступа посетителей и работников в отдельные помещения и к отдельным ИР, а также предотвращения вандализма и несанкционированных действий, ведущих к нарушению её работы, повреждению или уничтожению материальных и технических ценностей, помещений и зданий;
- 3) установка устройств, систем и (или) комплексов пожарной и охранной сигнализации.

- К инженерно-техническим средствам защиты относятся:
- ● специальное укрепление зданий и помещений;
- ● хранилища;
- ● системы пассивной безопасности (двери и металлоконструкции, замки, защитные стёкла, витрины и стенды, сейфы и металлические шкафы; преграждающие, ограждающие и запирающие устройства, ворота);
- ● средства индивидуальной защиты.

- Мероприятия по защите работников и посетителей организаций от различных несанкционированных воздействий на них включают:
- 1) создание физической защиты внутри зданий и помещений;
- 2) организацию охраны человеческих (одновременно и материально-технических) ресурсов;
- 3) установку внутри и вне здания различных технических защитных устройств, систем и (или) комплексов пожарной и охранной сигнализации;
- 4) обеспечение организации необходимыми индивидуальными средствами защиты органов дыхания, перчатками, сапогами и другой специальной одеждой;

- 5) проведение с персоналом, а порой и посетителями, мероприятий по:
- а) обучению их правилам пользования различными защитными средствами (в том числе первичными средствами пожаротушения);
- б) принятию соответствующих мер, эвакуации человеческих и материально-технических ресурсов при стихийных бедствиях, пожарах, нарушениях работоспособности инженерных сооружений (водо-, тепло- и электроснабжения, канализации);
- в) ознакомлению с правилами поведения в непредвиденных обстоятельствах

5. Охрана объектов с целью ограничения свободного доступа, смарткарты и др.

- Управление доступом служит для контроля входа/выхода через автоматические проходные (турникеты ,арочные металодетекторы) работников и посетителей организации. Контроль их перемещения осуществляется с помощью систем видеонаблюдения. В управление доступом входят также устройства и (или) системы ограждения для ограничения входа на территорию (охрана периметров).

- В качестве устройств, ограничивающих вход, обычно используют турникеты поясного типа. Для упорядочения потока посетителей применяют турникеты с перекрытием проёма в полный рост, обеспечивающих проход в двух направлениях в местах с напряжённым людским потоком.
- При этом используются метод визуализации (предъявления вахтёру удостоверения или других соответствующих документов) и автоматической идентификации входящих/выходящих работников и посетителей. Арочные металодетекторы позволяют выявлять несанкционированный внос/вынос металлизированных предметов и маркированных документов.

- Автоматизированные системы управления доступом позволяют работникам и посетителям, пользуясь персональными или разовыми электронными пропусками, проходить через проходную здания организации, заходить в разрешённые помещения и подразделения. Они используют контактный или бесконтактный способ идентификации. К мерам, обеспечивающим сохранность традиционных и нетрадиционных носителей информации и, как следствие, самой информации относят технологии штрихового кодирования. Это достаточно известная технология широко используется при маркировке различных товаров, в том числе документов, книг и журналов.

- В организациях используют удостоверения, пропуска, читательские билеты и т.п., в том числе пластиковые карты или ламинированные карточки, содержащие идентифицирующие пользователей штрих-коды. Эти документы с внесёнными в них штрих-кодами могут создаваться с помощью специальных печатающих устройств. Другой способ заключается в переносе штрих-кодов на существующие документы. Для этого используют специальные наклейки (этикетки) с уникальными штрих- кодами.

- Ламинирование – плёночное покрытие документов, защищающее их от лёгких механических повреждений и загрязнения, осуществляется с помощью пакетных ламинаторов, позволяющих обрабатывать документы размером от визитной карточки (порядка 50х75 мм) до формата А3

- Для проверки штрих-кодов используются сканирующие устройства считывания бар-кодов – сканеры. Они преобразуют считанное графическое изображение штрихов в цифровой код. При использовании контрольного кода, сканер вычисляет контрольный разряд и сравнивает его со считанным графическим изображением. Совпадение считанного и вычисленного контрольных разрядов означает правильное считывание штрихового кода. Сканер сообщает об этом световым и звуковым сигналом. В противном случае сигналы не выдаются.

- Для печатания штриховых кодов используются принтеры этикеток и обычные лазерные принтеры со специальным программным обеспечением. Первые обладают различными способами нанесения изображений (лазерные, термо- и термотрансферные и др.). Наибольшее распространение получили термотрансферные принтеры, в которых изображение переносится со специальной термотрансферной ленты под воздействием нагрева на бумагу или этикеточную ленту с липкой основой. Они также позволяют наносить цветное изображение, печать сложные этикетки с логотипом и даже цветными фотографиями.
- Кроме удобства, штрих-коды обладают и отрицательными качествами: дороговизна используемой технологии, расходных материалов и специальных программно-технических средств; отсутствие механизмов полной защиты документов от стирания, пропажи и др.

- С целью предоставления возможности отдельным индивидам проходить в соответствующие здания и помещения, а также пользоваться ИР применяют контактные и бесконтактные пластиковые и иные магнитные и электронные карты памяти, а также биометрические системы

- С их помощью можно ограничить вход в служебные помещения, а также возможность работы на технических устройствах несанкциониро- ванных пользователей. Для этого используют специальные устройства, позволяющие надёжно идентифицировать личность при считывании смарткарт. Кроме того, с этой же целью можно использовать электронные визитные карты на компакт-дисках.
- На прозрачном или цветном фоне лицевой стороны такой карты наносятся те же сведения, что и на обычной «визитке» (логотип и реквизиты). Физически – это часть компакт- диска диаметром 120 или 80 мм.

- Считыватели обеспечивают считывание идентификационного кода и передачу его в контроллер. Они преобразуют уникальный код пользователя в код стандартного формата, передаваемый контроллеру для принятия управленческого решения. Они могут фиксировать время прохода или открывания дверей и др.

- Наиболее чётко обеспечивают защиту данных на любом объекте средства идентификации личности, базирующиеся на использовании биометрических систем. Понятие «биометрия» — определяет раздел биологии, занимающийся количественными биологическими экспериментами с привлечением методов математической статистики. Это научное направление появилось в конце XIX века. Биометрия представляет совокупность автоматизированных методов и средств идентификации человека, основанных на его физиологических или поведенческих характеристиках.
- Биометрическая идентификация позволяет идентифицировать индивида по присущим ему специфическим биометрическим признакам, то есть его статическими (отпечаткам пальцев, роговице глаза, форме руки, генетическому коду, запаху и др.) и динамическими (голосу, почерку, поведению и др.) характеристиками.

- Уникальные биологические, физиологические и поведенческие характеристики, индивидуальные для каждого человека, называют биологическим кодом человека. Первые биометрические системы использовали рисунок (отпечаток) пальца. Заметим, что примерно 1 тыс. лет до н.э. в Китае и Вавилоне существовало представление об уникальности отпечатков пальцев, которые ставили под юридическими документами, но дактилоскопию стали применять в Англии в 1897 году, а в США – в 1903 году.

- Преимущество таких систем идентификации, по сравнению с традиционными (например, PIN-кодовыми, доступом по паролю), заключается в идентификации не внешних предметов, принадлежащих человеку, а самого человека. Анализируемые характеристики человека невозможно утерять, передать, забыть и крайне сложно подделать. Они практически не подвержены износу и не требуют замены или восстановления. Это обстоятельство послужило основанием в различных странах (в том числе России) для включения биометрических признаков в загранпаспорта и другие официальные идентифицирующие личности документы.

- Биометрическая идентификация считается одним из наиболее надёжных способов. Многие зарубежные организации для обеспечения физической и информационной безопасности перешли на биометрические системы. В биометрических системах используют технологии машинного зрения для распознавания личности по: отпечаткам пальцев, геометрии лица, кисти руки или рисунка вен, рисунку радужной оболочки или сетчатке глаза, голосу, почерку и др.

- С помощью этих технологий осуществляются:
- 1) ограничение доступа к информации и обеспечение персональной ответственности за её сохранность;
- 2) обеспечение допуска сертифицированных специалистов;
- 3) предотвращение проникновения злоумышленников на охраняемые территории и в помещения вследствие подделки и (или) кражи документов (карт, паролей);
- 4) организация учёта доступа и посещаемости сотрудников, а также решается ряд других проблем.

- Одной из главных мер защиты от утечки информации в компьютерных сетях является установление специальных технических средств, которые называются Firewalls (в переводе с английского это звучит как «огненная стена»). Часто под этим термином подразумевают «противопожарные перегородки», «защитный барьер» или брандмауэр. Их назначение заключается в воспрепятствовании проникновению злоумышленника в информацию на носителях пользователя, то есть внешняя защита. Это устройство располагают между внутренней локальной сетью организации и Интернетом для ограничения трафика, пресечения попыток несанкционированного доступа к внутренним ресурсам организации.

- Современные брандмауэры выполняют также функции «отсечения» от пользователей корпоративных сетей незаконной и нежелательной для них корреспонденции, передаваемой по электронной почте, ограничивая, таким образом, возможность получения избыточной информации и так называемого «мусора» (спама).