**ПРАВОВАЯ ОХРАНА ПРОГРАММ И ДАННЫХ. ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ.**

**Цель урока: Знать что такое защита информации; Информационная безопасность; Меры предотвращения.**

**План урока:**

**Защита информации** – это деятельность по предотвращению утраты и утечки защищаемой информации.

**Информационной безопасностью** называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода.

Информационная безопасность дает гарантию того, что достигаются следующие **цели**:

· конфиденциальность критической информации;

· целостность информации и связанных с ней процессов (создания, ввода, обработки и вывода);

· доступность информации, когда она нужна;

· учет всех процессов, связанных с информацией.

Существует четыре уровня защиты компьютерных и информационных ресурсов:

**Предотвращение** предполагает, что только авторизованный персонал имеет доступ к защищаемой информации и технологии.

**Обнаружение** предполагает раннее раскрытие преступлений и злоупотреблений, даже если механизмы защиты были обойдены.

**Ограничение** уменьшает размер потерь, если преступление все-таки произошло, несмотря на меры по его предотвращению и обнаружению.

**Восстановление** обеспечивает эффективное воссоздание информации при наличии документированных и проверенных планов по восстановлению.

**Меры защиты** - это меры, вводимые руководством, для обеспечения безопасности информации. К мерам защиты относят разработку административных руководящих документов, установку аппаратных устройств или дополнительных программ, основной целью которых является предотвращение преступлений и злоупотреблений.

Формирование режима информационной безопасности - проблема комплексная. Меры по ее решению можно разделить на **четыре уровня**:

1. - **законодательный:** законы, нормативные акты, стандарты и т. п.;
2. - **административный:** действия общего характера, предпринимаемые руководством организации;
3. - **процедурный:** конкретные меры безопасности, имеющие дело с людьми;
4. - **программно-технический:** конкретные технические меры.

меры защиты:

**Аутентификация пользователей**: пароль. Существуют также различные устройства для идентификации личности по биометрической информации - по радужной оболочке глаза, отпечаткам пальцев, размерам кисти руки и т.д.

**2. Защита пароля.**

Следующие правила полезны для защиты пароля:

· нельзя делится своим паролем ни с кем;

· пароль должен быть трудно угадываемым;

· для создания пароля нужно использовать строчные и прописные буквы.

· не рекомендуется использовать пароль, который является адресом, псевдонимом, именем родственника, телефонным номером или чем-либо очевидным;

· предпочтительно использовать длинные пароли, так как они более безопасны, лучше всего, чтобы пароль состоял из 6 и более символов;

· пароль не должен отображаться на экране компьютера при его вводе;

· пароли должны отсутствовать в распечатках;

· нельзя записывать пароли на столе, стене или терминале, его нужно держать в памяти;

· пароль нужно периодически менять и делать это не по графику;

· на должности администратора паролей должен быть самый надежный человек;

· не рекомендуется использовать один и тот же пароль для всех сотрудников в группе;

· когда сотрудник увольняется, необходимо сменить пароль;

**3. Процедуры авторизации.**

В организации, имеющей дело с критическими данными, должны быть разработаны и внедрены процедуры авторизации, которые определяют, кто из пользователей должен иметь доступ к той или иной информации и приложениям.

В организации должен быть установлен такой порядок, при котором для использования компьютерных ресурсов, получения разрешения доступа к информации и приложениям, и получения пароля требуется разрешение тех или иных начальников.

Если информация обрабатывается на большом вычислительном центре, то необходимо контролировать физический доступ к вычислительной технике. Могут оказаться уместными такие методы, как журналы, замки и пропуска, а также охрана. Ответственный за информационную безопасность должен знать, кто имеет право доступа в помещения с компьютерным оборудованием и выгонять оттуда посторонних лиц.

**4. Предосторожности при работе.**

Рекомендуется:

· отключать неиспользуемые терминалы;

· закрывать комнаты, где находятся терминалы;

· разворачивать экраны компьютеров так, чтобы они не были видны со стороны двери, окон и прочих мест, которые не контролируются;

· установить специальное оборудование, ограничивающее число неудачных попыток доступа, или делающее обратный звонок для проверки личности пользователей, использующих телефоны для доступа к компьютеру

· использовать программы отключения терминала после определенного периода неиспользования;

· выключать систему в нерабочие часы;

· использовать системы, позволяющие после входа пользователя в систему сообщать ему время его последнего сеанса и число неудачных попыток установления сеанса после этого. Это позволит сделать пользователя составной частью системы проверки журналов.

**5. Физическая безопасность.**

В защищаемых компьютерных системах необходимо принимать меры по предотвращению, обнаружению и минимизации ущерба от пожара, наводнения, загрязнения окружающей среды, высоких температур и скачков напряжения.

Пожарная сигнализация и системы пожаротушения должны регулярно проверяться. ПЭВМ можно защитить с помощью кожухов, чтобы они не были повреждены системой пожаротушения. Горючие материалы не должны храниться в этих помещениях с компьютерами.

Температура в помещении может контролироваться кондиционерами и вентиляторами, а также хорошей вентиляцией в помещении. Проблемы с чрезмерно высокой температурой могут возникнуть в стойках периферийного оборудования или из-за закрытия вентиляционного отверстия в терминалах или ПЭВМ, поэтому необходима их регулярная проверка.

Желательно применение воздушных фильтров, что поможет очистить воздух от веществ, которые могут нанести вред компьютерам и дискам. Следует запретить курить, принимать пищу и пить возле ПЭВМ.

Компьютеры должны размещаться как можно дальше источников большого количества воды, например трубопроводов.

**6. Защита носителей информации** **(исходных документов, лент, картриджей, дисков, распечаток).**

Для защиты носителей информации рекомендуется:

· вести, контролировать и проверять реестры носителей информации;

· обучать пользователей правильным методам очищения и уничтожения носителей информации;

· делать метки на носителях информации, отражающие уровень критичности содержащейся в них информации;

· уничтожать носители информации в соответствии с планом организации;

· доводить все руководящие документы до сотрудников;

· хранить диски в конвертах, коробках, металлических сейфах;

· не касаться поверхностей дисков, несущих информацию

· осторожно вставлять диски в компьютер и держать их подальше от источников магнитного поля и солнечного света;

· убирать диски и ленты, с которыми в настоящий момент не ведется работа;

· хранить диски разложенными по полкам в определенном порядке;

· не давать носители информации с критической информацией неавторизованным людям;

· выбрасывать или отдавать поврежденные диски с критической информацией только после их размагничивания или аналогичной процедуры;

· уничтожать критическую информацию на дисках с помощью их размагничивания или физического разрушения в соответствии с порядком в организации;

· уничтожать распечатки и красящие ленты от принтеров с критической информацией в соответствии с порядком организации;

· обеспечить безопасность распечаток паролей и другой информации, позволяющей получить доступ к компьютеру.

**7. Выбор надежного оборудования.**

Производительность и отказоустойчивость информационной системы во многом зависит от работоспособности серверов. При необходимости обеспечения круглосуточной бесперебойной работы информационной системы используются специальные отказоустойчивые компьютеры, т. е. такие, выход из строя отдельного компонента которых не приводит к отказу машины.

На надежности информационных систем отрицательно сказываются и наличие устройств, собранных из комплектующих низкого качества, и использование нелицензионного ПО. Чрезмерная экономия средств на обучение персонала, закупку лицензионного ПО и качественного оборудования приводит к уменьшению времени безотказной работы и значительным затратам на последующее восстановление системы.

**8. Источники бесперебойного питания.**

Компьютерная система энергоемка, и потому первое условие ее функционирования - бесперебойная подача электроэнергии. Необходимой частью информационной системы должны стать источники бесперебойного питания для серверов, а по возможности, и для всех локальных рабочих станций. Рекомендуется также дублировать электропитание, используя для этого различные городские подстанции. Для кардинального решения проблемы можно установить резервные силовые линии от собственного генератора организации.

**9. Разработка адекватных планов обеспечения непрерывной работы и восстановления.**

Целью планов обеспечения непрерывной работы и восстановления являются гарантии того, что пользователи смогут продолжать выполнять свои самые главные обязанности в случае невозможности работы по информационной технологии. Обслуживающий персонал должен знать, как им действовать по этим планам.

Планы обеспечения непрерывной работы и восстановления (ОНРВ) должны быть написаны, проверены и регулярно доводиться до сотрудников. Процедуры плана должны быть адекватны уровню безопасности и критичности информации. План ОНРВ может применяться в условиях неразберихи и паники, поэтому нужно регулярно проводить тренировки сотрудников.

**10. Резервное копирование.**

Одним из ключевых моментов, обеспечивающих восстановление системы при аварии, является резервное копирование рабочих программ и данных. В локальных сетях, где установлены несколько серверов, чаще всего система резервного копирования устанавливается непосредственно в свободные слоты серверов. В крупных корпоративных сетях предпочтение отдается выделенному специализированному архивационному серверу, который автоматически архивирует информацию с жестких дисков серверов и рабочих станций в определенное время, установленное администратором сети, выдавая отчет о проведенном резервном копировании.

Для архивной информации, представляющей особую ценность, рекомендуется предусматривать охранное помещение. Дубликаты наиболее ценных данных, лучше хранить в другом здании или даже в другом городе. Последняя мера делает данные неуязвимыми в случае пожара или другого стихийного бедствия.

**11. Дублирование, мультиплексирование и резервирование офисов.**

Помимо резервного копирования, которое производится при возникновении внештатной ситуации либо по заранее составленному расписанию, для большей сохранности данных на жестких дисках применяют специальные технологии - зеркалирование дисков и создание RAID-массивов, которые представляют собой объединение нескольких жестких дисков. При записи информация поровну распределяется между ними, так что при выходе из строя одного из дисков находящиеся на нем данные могут быть восстановлены по содержимому остальных.

Технология кластеризации предполагает, что несколько компьютеров функционируют как единое целое. Кластеризуют, как правило, серверы. Один из серверов кластера может функционировать в режиме горячего резерва в полной готовности начать выполнять функции основной машины в случае ее выхода из строя. Продолжением технологии кластеризации является распределенная кластеризация, при которой через глобальную сеть объединяются несколько кластерных серверов, разнесенных на большое расстояние.

Распределенные кластеры близки к понятию резервных офисов, ориентированных на обеспечение жизнедеятельности предприятия при уничтожении его центрального помещения. Резервные офисы делят на холодные, в которых проведена коммуникационная разводка, но отсутствует какое-либо оборудование и горячие, которыми могут быть дублирующий вычислительный центр, получающий всю информацию из центрального офиса, филиал, офис на колесах и т.д.

**12. Резервирование каналов связи.**

При отсутствии связи с внешним миром и своими подразделениями, офис оказывается парализованным, потому большое значение имеет резервирование внешних и внутренних каналов связи. При резервировании рекомендуется сочетать разные виды связи - кабельные линии и радиоканалы, воздушную и подземную прокладку коммуникаций и т.д.

По мере того, как компании все больше и больше обращаются к Internet, их бизнес оказывается в серьезной зависимости от функционирования Internet-провайдера. У поставщиков доступа к Сети иногда случаются достаточно серьезные аварии, поэтому важно хранить все важные приложения во внутренней сети компании и иметь договора с несколькими местными провайдерами. Следует также заранее продумать способ оповещения стратегических клиентов об изменении электронного адреса и требовать от провайдера проведения мероприятий, обеспечивающих оперативное восстановление его услуг после аварий.

**12. Защита данных от перехвата.**

Для любой из трех основных технологий передачи информации существует технология перехвата: для кабельных линий - подключение к кабелю, для спутниковой связи – использование антенны приема сигнала со спутника, для радиоволн - радиоперехват. Российские службы безопасности разделяют коммуникации на три класса. Первый охватывает локальные сети, расположенные в зоне безопасности, т. е. территории с ограниченным доступом и заэкранированным электронным оборудованием и коммуникационными линиями, и не имеющие выходов в каналы связи за ее пределами. Ко второму классу относятся каналы связи вне зоны безопасности, защищенные организационно-техническими мерами, а к третьему - незащищенные каналы связи общего пользования. Применение коммуникаций уже второго класса значительно снижает вероятность перехвата данных.

Для защиты информации во внешнем канале связи используются следующие устройства: скремблеры для защиты речевой информации, шифраторы для широковещательной связи и криптографические средства, обеспечивающие шифрование цифровых данных.