# ЗАЩИТА ПРОГРАММНЫХ ПРОДУКТОВ. ВИДЫ ИНФОРМАЦИОННОЙ ОПАСНОСТИ

**Вопросы и задания для конспекта**

1. **Что понимают под безопасностью информации?**
2. **Доступность информации – это ...**
3. **Перечислить юридические средства и методы защиты**
4. **Перечислить административные средства и методы защиты**
5. **Перечислить технические средства и методы защиты**
6. **Как организуют защиту электронных данных, хранящихся на различных носителях?**
7. **Какие методы используют для обеспечения санкционированным лицам доступа к объектам и информационным ресурсам (перечислить)?**
8. **Для чего нужна аутентификация?**
9. **Для чего нужна авторизация?**
10. **Для чего нужна идентификация?**
11. **Основные угрозы безопасности (перечислить).**
12. **В чем заключается угроза нарушения конфиденциальности?**
13. **В чем заключается угроза нарушения целостности?**
14. **В чем заключается угроза нарушения доступности?**
15. **Каналы утечки информации – это ...**
16. **Дать краткую характеристику каналам утечки информации:**
    a. **электромагнитные;**
    b. **электрические;**
    c. **индукционные;**
    d. **акустические;**
    e. **каналам утечки видовой информации.**

---

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.

Доступ в АИС – получение возможности ознакомления с информацией, ее обработки и воздействия на информацию и ресурсы автоматизированной информационной системы с использованием программных и технических средств.

Доступность (информации [ресурсов АИС]) – состояние информации (ресурсов АИС), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно. К правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации, а также права на изменение, использование, уничтожение ресурсов.

Средства и методы защиты информации обычно делят на две большие группы: организационные и технические. Под организационными подразумеваются: юридические средства; административные средства; технические средства.

Юридические средства:

- Статья 272 – Неправомерный доступ к компьютерной информации;
- Статья 273 – Создание, использование и распространение вредоносных программ для ЭВМ;
- Статья 274 – Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети;
- «Закон об авторском праве и смежных правах»
- «Закон о правовой охране программ для ЭВМ и баз данных»

Административные средства:

- Меры по внедрению и активному использованию технических средств предупреждения;
- Правила, ограничивающие свободу действий пользователей;
- Обучение неквалифицированных пользователей;
- Меры по упорядочиванию информационных потоков в корпоративной сети и прав доступа

Технические средства:

- Системы разграничения доступа;
- Криптографические средства;
- Антивирусные мониторы, фильтры, сканеры;
- Межсетевые экраны (брандмауэры);
- Средства обеспечения отказоустойчивости и резервного копирования.

Под техническими – аппаратные, программные и криптографические мероприятия, направленные на обеспечение защиты объектов, людей и информации.

Защита носителей информации.

Одной из важных проблем информационной безопасности является организация защиты электронных данных, хранящихся на различных носителях.

Обеспечение сохранности информации производится путём применения специальных мер организации хранения, восстановления (регенерации) информации, специальных устройств резервирования. Качество обеспечения сохранности информации зависит от её целостности (точности, полноты) и готовности к постоянному использованию.

Специалисты предлагают несколько методик обеспечения сохранности электронных данных вообще и в Интернете в частности. Среди них перезапись; архивирование; защита от несанкционированного использования, замены, искажения и удаления; защита от компьютерных вирусов и неполадок в электрических и компьютерных сетях.

Под термином «архив» понимается совокупность данных, организованная на носителях (в т.ч. электронных) информации с целью обеспечения в случае необходимости их дальнейшего использования. Архивы зачастую организуются путём создания копий имеющихся оригиналов.

Электронный архив – файл, содержащий один или несколько файлов в сжатой или несжатой форме и информацию, связанную с этими файлами.

Копирование электронной информации означает создание дубликатов имеющихся электронных данных. При этом полученные копии занимают столько же места, сколько и исходные файлы, что нерационально с точки зрения хранения огромных массивов копий файлов.

Для решения этой проблемы используют специальные программы архивации файлов (ZIP, ARJ, RAR, а также WINZIP, WINRAR и др.). Они позволяют не только сэкономить место на электронных носителях информации, но и объединять группы совместно используемых файлов в один архивный файл, обеспечивая надёжное и быстрое копирование электронных данных.

Архивация электронных данных подразумевает организацию рабочих, резервных и страховых архивов. Наличие трёх видов архивов обусловлено существованием разных, с точки зрения потребности хранения и сохранения, видов информации: оперативные данные, условно-постоянная, постоянная (страховая) и другая информация.

Оперативные данные характеризуются значительной, по сравнению с условно-постоянными, скоростью изменения своих параметров (объёма, содержания и др.) и требуют более частого обновления копий. Они имеют короткий период перезаписи и хранения (шаг копирования).

Рабочие архивы служат для ручной или автоматической записи создаваемых постоянных или временных (оперативных) данных. В дальнейшем эта информация может не использоваться или перейти в разряд долговременно хранящихся данных. Рабочие архивы рекомендуется создавать и актуализировать непосредственно по окончании ввода порции данных или смены. Они формируются на технологические материалы и БД, подготавливаемые, редактируемые и оперативные документы и создаются в отдельных каталогах на данном или другом компьютере, сервере и, как правило, на перезаписываемых внешних носителях данных.

Для быстрого восстановления работоспособности системы в случае возникновения аварийной ситуации предварительно создают резервные копии файлов – резервные архивы. Такой процесс называется резервным копированием (англ. «Backup”, «Cheekpoint”). Он выполняется

автоматическим или ручным способом. Ручное резервное копирование осуществляют периодически уполномоченные сотрудники в соответствии с принятыми в организациях правилами. Автоматическое резервное копирование производят с учётом тех же правил, но специальными программами (например «Backup”), в том числе вовремя отсутствия сотрудников на своих рабочих местах.

Для восстановления информации в случае утраты или порчи основных машиночитаемых данных и резервных копий, а также для длительного хранения электронных данных в месте, защищённом от вредных воздействий и несанкционированного доступа, используют страховое (архивное) копирование, с помощью которого создают страховые архивы. Создание страховых архивов – формирование архивных копий файлов, предназначенных для долговременного или бессрочного хранения.

Носители, на которых они хранятся, называют архивными. Такой процесс предполагает более строгое структурирование информации, высокую степень автоматизации архивирования и восстановления данных, а также работу с большими объёмами информации.

Периодическое проведение архивного копирования позволяет иметь копии нескольких разных версий одних и тех же файлов.

Современные способы сохранения электронных данных предполагают применение названных и иных методов хранения электронной информации. С этой целью, кроме носителей электронных данных, используют дублирование данных с помощью технологий «Backup”, «зеркалирования”, создания высоконадёжных локальных и сетевых хранилищ данных и др.

Используются различные методы, обеспечивающие санкционированным лицам доступ к объектам и информационным ресурсам. К ним относят аутентификацию и идентификацию пользователей.

Аутентификация – метод независимого от источника информации установления подлинности информации на основе проверки подлинности её внутренней структуры («это тот, кем назвался?»).

Авторизация – в информационных технологиях это предоставление определённых полномочий лицу или группе лиц на выполнение некоторых действий в системе обработки данных («имеет ли некто право выполнять данную деятельность?»). Посредством авторизации устанавливаются и реализуются права доступа к ресурсам.

Идентификация – это метод сравнения предметов или лиц по их характеристикам, путём опознавания по предметам или документам, определения полномочий, связанных с доступом лиц в помещения, к документам и т. д. («это тот, кем назвался и имеет право выполнять данную деятельность?»).

Проверка подлинности пользователя компьютера или компьютерной программы обычно осуществляется операционной системой. Пользователь идентифицируется своим именем, а средством аутентификации служит пароль. Для эффективного использования этих методов, кроме физических мер охраны объектов, широко применяются программно-технические средства, основанные на использовании биометрических систем, криптографии.

Угрозы безопасности: угроза нарушения конфиденциальности; угроза нарушения целостности; угроза нарушения доступности.

Угроза нарушения конфиденциальности. Заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Иногда, в связи с угрозой нарушения конфиденциальности, используется термин «утечка».

Угроза нарушения целостности. Предполагает любое незапланированное и несанкционированное изменение информации, хранящейся в системе или передаваемой из одной системы в другую.

Санкционированными изменениями считаются те, которые сделаны уполномоченными лицами с обоснованной целью. Целостность может быть нарушена в результате преднамеренных действий человека, а также - в результате возникновения случайной ошибки программного или аппаратного обеспечения.

Угроза нарушения доступности. Возникает всякий раз, когда в результате некоторых событий (преднамеренных действий или ошибки) блокируется доступ к некоторому ресурсу вычислительной системы.

Блокирование может быть постоянным – запрашиваемый ресурс никогда не будет получен, или оно может вызывать только задержку выдачи ресурса, достаточно долгую для того, чтобы он стал бесполезным.

## КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ В ИС

**Каналы утечки информации** – это методы и пути утечки информации из информационной системы; паразитная (нежелательная) цепочка носителей информации, один или несколько из которых являются (могут быть) правонарушителем или его специальной аппаратурой. Играют основную роль в защите информации, как фактор информационной безопасности.

***Электромагнитные каналы*** утечки информации формируются в результате побочного электромагнитного излучения: элементов технические средства обработки информации (ТСОИ), сигнал которых (электроток, напряжение, частота и фаза) изменяется так же, как и информационный; ВЧ-генераторов ТСОИ и вспомогательные технические средства обработки информации (ВТСОИ), излучение которых может непреднамеренно модулироваться электрическим сигналом, наведенным информационным; ВЧ-усилителей ТСПИ в результате случайного преобразования отрицательной обратной связи в паразитную положительную, что может привести к самовозбуждению и переходу усилителя из режима усиления в режим автогенерации сигналов, модулированных информационным сигналом.

***Электрические каналы*** утечки информации появляются вследствие наводки электромагнитного излучения, возникающего при передаче информационных сигналов элементами ТСОИ, а также из-за наличия гальванической связи между соединительными линиями ТСОИ и другими проводниками или линиями ВТСОИ; информационных сигналов в цепи электропитания вследствие магнитной связи между выходным трансформатором усилителя и трансформатором системы электропитания, а также неравномерной нагрузки выпрямителя, приводящей к изменению потребляемого тока в соответствии с изменениями информационного сигнала; наводки информационных сигналов в цепи заземления за счет гальванической связи с землей различных проводников, в том числе нулевого провода сети электропитания, а также металлических конструкционных элементов, расположенных за границей контролируемой зоны безопасности. Кроме того, электрические каналы утечки могут возникать в результате съема информации с помощью различных аппаратных или так называемых закладных устройств, например мини-передатчиков.

Излучение этих устройств, устанавливаемых в ТСОИ, модулируется информационным сигналом и принимается специальными устройствами за пределами контролируемой зоны. Возможно применение специального ВЧ-облучения, т.е. создание электромагнитного поля, которое взаимодействует с элементами ТСОИ и модулируется информационным сигналом. Это так называемый параметрический канал утечки информации. Особую опасность представляет перехват информации при передаче по каналам связи, поскольку и этом случае возможен свободный несанкционированный доступ к передаваемым данным.

Часто используют ***индукционный канал*** перехвата. Современные индукционные датчики способны снимать информацию не только с изолированных кабелей, но и с кабелей, защищенных двойной броней стальной ленты и стальной проволоки.

Среди каналов утечки акустической информации различают воздушные, вибрационные, электроакустические, оптоэлектронные и параметрические. В широко распространенных воздушных каналах для перехвата информации используются высокочувствительные и направленные акустические закладки, например микрофоны, соединенные с диктофонами или специальными мини-передатчиками. Перехваченная закладами акустическая информация может передаваться по радиоканалам, или переменного тока, соединительным линиям, проложенным в помещении проводникам, трубам и т. п. Для приема информации, как правило, используются специальные устройства. Особый интерес представляют закладные устройства, устанавливаемые либо непосредственно в корпус телефонного аппарата, либо подключаемые к линии в телефонной розетке. Подобные приборы, в конструкцию которых входят микрофон и блок коммутации, часто называют «телефонным ухом».

При поступлении в линию кодированного сигнала вызова или при дозвоне к контролируемому телефону по специальной схеме блок коммутации подключает к линии микрофон и обеспечивает передачу информации (обычно речевой) на неограниченное расстояние.

В вибрационных (или структурных) каналах средой распространения информации являются конструктивные элементы зданий (стены, потолки, полы и др.), а также трубы вода и теплоснабжения, канализации.

***Электроакустические каналы*** формируются в результате преобразования акустических сигналов в электрические путем «высокочастотного навязывания» или перехвата с помощью ВТСОИ. Канал утечки первого типа возникает в результате несанкционированного ввода в линии сигнала ВЧ-генератора, функционально связанного с элементами ВТСОИ, и модуляции его информационным сигналом. В этом случае для перехвата разговоров, ведущихся в помещении, чаще всего используют телефонный аппарат с выходом за пределы контролируемой зоны. Кроме того, некоторые ВТСОИ, например датчики систем противопожарной сигнализации, громкоговорители ретрансляционной сети и т.п., могут и сами содержать электроакустические преобразователи. Перехватить акустические сигналы можно, подключив такие средства к соединительной линии телефонного аппарата с электромеханическим звонком и прослушав при не снятой с рычага трубке разговоры, ведущиеся в помещении (так называемый микрофонный эффект).

Облучая лазерным пучком вибрирующие в акустическом поле тонкие отражающие поверхности (стекла окон, зеркала, картины и т. п.), можно сформировать *оптоэлектронный (лазерный)* канал утечки акустической информации. Отраженное лазерное излучение, модулированное акустическим сигналом по амплитуде и фазе, демодулируется приемником, который и идентифицирует речевую информацию.

Средства перехвата – локационные системы, работающие, как правило, в ИК-диапазоне и известные как «лазерные микрофоны». Дальность их действия – несколько сотен метров.

При воздействии акустического поля на элементы ВЧ-генераторов и изменении взаимного расположения элементов систем, проводов, дросселей и т. п. передаваемый сигнал модулируется информационным. В результате формируется параметрический канал утечки акустической информации. Модулированные ВЧ-сигналы перехватываются соответствующими средствами. Параметрический канал утечки создается и путем «ВЧ-облучения» помещения, где установлены полуактивные закладные устройства, параметры которых изменяются в соответствии с изменениями акустического сигнала.

По каналам утечки акустической информации могут перехватываться не только речевые сигналы. Известны случаи статистической обработки акустической информации принтера или клавиатуры с целью перехвата компьютерных текстовых данных. Такой способ позволяет снимать информацию и по системе централизованной вентиляции.

В последнее время большое внимание уделяется *каналам утечки видовой информации*, по которым получают изображения объектов или копий документов.

Для этих целей используют оптические приборы (бинокли, подзорные трубы, телескопы, монокуляры), телекамеры, приборы ночного видения, тепловизоры и т. п. Для снятия копий документов применяют электронные и специальные закамуфлированные фотоаппараты, а для дистанционного съема видовой информации – видеозакладки. Наиболее распространены следующие средства защиты от утечки видовой информации: ограничение доступа, техническая (системы фильтрации, шумоподавления) и криптографическая защита, снижение уровня паразитных излучений технических средств, охрана и оснащение средствами тревожной сигнализации.

Весьма динамично сейчас развиваются компьютерные методы съема информации. Хотя здесь также применяются разнообразные закладные устройства, несанкционированный доступ, как правило, получают с помощью специальных программных средств (компьютерных вирусов, «троянских коней», программных закладок и т. п.). Особенно много неприятностей доставляют компьютерные вирусы – в настоящее время известно свыше нескольких десятков тысяч их модификаций.