Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Кафедра Конструирования и производства радиоэлектронных средств

Дисциплина: «САПР технологических процессов производства электронных средств»

ТЕМА 8: Основы защиты информации в САПР

Лекция № 12. Общие принципы защиты информации в САПР

(2 часа)

Доцент кафедры, к.п.н.,

Мордовин В.Н.

2018 г.

СПб ГУТ)))

Учебные вопросы

1. Основные понятия.
2. Виды угроз безопасности в САПР.
3. Методы и средства защиты информации.

Литература

СПЕЦИАЛЬНЫЕ ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ (СТР-К) . М. 2001.

Баранов В.М. и др. Организация защиты информации. Учебное пособие. СПб, ВКА им.А.Ф.Можайского. 2015.

ВВЕДЕНИЕ

Различные субъекты по отношению к определенной информации могут выступать *в качестве* (возможно одновременно):

- источников (поставщиков) информации;
- пользователей (потребителей) информации;
- собственников (владельцев, распорядителей) информации;
- физических и юридических лиц, о которых собирается информация;
- владельцев систем сбора и обработки информации и участников процессов обработки и передачи информации и т.д.

Для успешного осуществления деятельности по управлению объектами некоторой предметной области субъекты информационных отношений *могут быть заинтересованы* в обеспечении:

- *своевременного доступа* к необходимой информации;
- *конфиденциальности* (сохранения в тайне) определенной части информации;
- *достоверности* (полноты, точности, адекватности, целостности) информации;
- *защиты от* навязывания ложной (недостоверной, искаженной) информации, т.е. от *дезинформации*;
- *защиты части информации от незаконного ее тиражирования* (защита авторских прав, прав собственника информации и т.п.);
- *разграничения законных прав* (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;
- *контроля и управления* процессами обработки и передачи информации.

Свойства информации и систем ее обработки:

- ***доступность*** информации, т.е. свойство системы в которой циркулирует информация, *характеризующаяся способностью обеспечивать своевременный беспрепятственный доступ субъектов* к интересующим их данным и готовностью соответствующих автоматизированных служб к выполнению поступающих от субъектов запросов;
- ***целостность*** информации, т.е. свойство информации, заключающееся в ее *существовании в неискаженном виде;*
- ***конфиденциальность*** информации - субъективно определяемая характеристика информации, указывающая на необходимость введения *ограничений на круг субъектов*, которые *имеют доступ к данной информации*.

1. Основные понятия

- ***Защита информации*** — это средства обеспечения безопасности информации.
- ***Безопасность информации*** — защита информации от утечки, модификации и утраты. *Сфера безопасности информации* — не защита информации, а *защита прав собственности* на нее и интересов субъектов информационных отношений.
- ***Утечка информации*** - ознакомление *постороннего лица* с содержанием секретной информации.
- ***Модификация информации*** — *несанкционированное изменение информации*, корректное по форме и содержанию, но *другое по смыслу*.
- ***Утрата информации*** — физическое *уничтожение* информации.
- ***Цель защиты информации*** — *противодействие угрозам* безопасности информации.

1. Основные понятия

- ***Угроза безопасности информации*** — *действие или событие*, которое может привести к *разрушению, искажению или несанкционированному использованию* информационных ресурсов (т.е. к утечке, модификации и утрате), включая хранимую, передаваемую и обрабатываемую информацию, а также программные и аппаратные средства.
- ***Система защиты*** — это совокупность (комплекс) специальных *мер правового (законодательного) и административного характера, организационных мероприятии, физических и технических (программно-аппаратных) средств защиты, а также специального персонала*, предназначенных для обеспечения безопасности информации, информационных технологий и автоматизированной системы в целом.

Для построения эффективной системы защиты необходимо провести следующие ***работы:***

1) определить угрозы безопасности информации;
2) выявить возможные каналы утечки информации и несанкционированного доступа (НСД) к защищаемым данным;
3) построить модель потенциального нарушителя;
4) выбрать соответствующие меры, методы, механизмы и средства защиты;
5) построить замкнутую, комплексную, эффективную систему защиты, проектирование которой начинается с проектирования самих АС и технологий.

При ***предпроектномм обследовании*** *объекта:*

- *устанавливается* наличие секретной (конфиденциальной) информации в разрабатываемой САПР, оценивается уровень ее конфиденциальности и объем;
- *определяются* режимы обработки информации (диалоговый, телеобработка и режим реального времени), состав комплекса технических средств и т.д.;
- *анализируется* возможность использования имеющихся на рынке сертифицированных средств ЗИ;
- *определяется степень участия* персонала, функциональных служб, специалистов и вспомогательных работников объекта автоматизации в обработке информации, характер их взаимодействия между собой и со службой безопасности;
- *определяются мероприятия* по обеспечению режима секретности на стадии разработки.

2. Виды угроз безопасности в САПР

Основными видами угроз безопасности информационных систем и информации (угроз интересам субъектов информационных отношений) являются:

- *стихийные* бедствия и аварии (наводнение, ураган, пожар и т.п.);
- *сбои и отказы* оборудования (технических средств) САПР;
- последствия *ошибок проектирования и разработки компонентов* САПР (аппаратных средств, технологии обработки информации, программ, структур данных и т.п.);
- *ошибки эксплуатации* (пользователей, операторов и другого персонала);
- *преднамеренные действия* нарушителей и злоумышленников (обиженных лиц из числа персонала, преступников, шпионов, диверсантов и т.п.).

Угрозы безопасности можно классифицировать по:

По результатам акции:

1*) угроза утечки;*

2) угроза модификации;

3) угроза утраты.

По нарушению свойств информации:

а*) угроза нарушения конфиденциальности обрабатываемой информации;*

б) угроза нарушения целостности обрабатываемой информации;

в) угроза нарушения работоспособности системы (отказ в обслуживании), т.е. угроза доступности.

По природе возникновения:

1*) естественные; 2) искусственные.*

- ***Естественные угрозы*** — это угрозы, вызванные воздействиями на САПР и ее элементы объективных физических процессов или стихийных природных явлений.

Основные непреднамеренные искусственные угрозы САПР (действия, совершаемые случайно, по незнанию, невнимательности или халатности, но без злого умысла):

1) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);

2) неправомерное включение оборудования или изменение режимов работы устройств и программ;

3) неумышленная порча носителей информации;

4) запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

5) нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

6) заражение компьютера вирусами;

7) неосторожные действия, приводящие к разглашению конфиденциальной информации или делающие ее общедоступной;

8) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);

9) проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ с возможностями, представляющими угрозу для работоспособности системы и безопасности информации;

- 10) игнорирование организационных ограничений (установленных правил) при ранге в системе;
- 11) вход в систему в обход средств зашиты (загрузка посторонней операционной системы со сменных носителей и т.п.);
- 12) некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
- 13) пересылка данных по ошибочному адресу абонента (устройства);
- 14) ввод ошибочных данных;
- 15) неумышленное повреждение каналов связи.

- Основные ***преднамеренные искусственные угрозы*** характеризуются возможными путями умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

а) физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);

б) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);

в) действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);

г) внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);

д) вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;

е) применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;

ж) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводка активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.);

з) перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;

и) хищение носителей информации (флэш-карт, микросхем памяти, запоминающих устройств и персональных ЭВМ);

к) несанкционированное копирование носителей информации;

л) хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);

м) чтение остатков информации из оперативной памяти и с внешних за-поминающих устройств;

н) чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме, используя недостатки мультизадачных операционных систем и систем программирования;

о) незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, имитации интерфейса системы и т.п.) с последующей маскировкой под зарегистрированного пользователя («маскарад»);

п) несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие, как номер рабочей станции в сети, адрес в системе связи, аппаратный блок кодирования и т.п.;

р) вскрытие шифров криптозащиты информации;

с) внедрение аппаратных спецвложений, программ «закладок» и «вирусов» («троянских коней» и «жучков»), т.е. таких участков программ, которые позволяют преодолеть систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации;

т) незаконное подключение к линиям связи с целью работы «между строк», с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;

у) незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

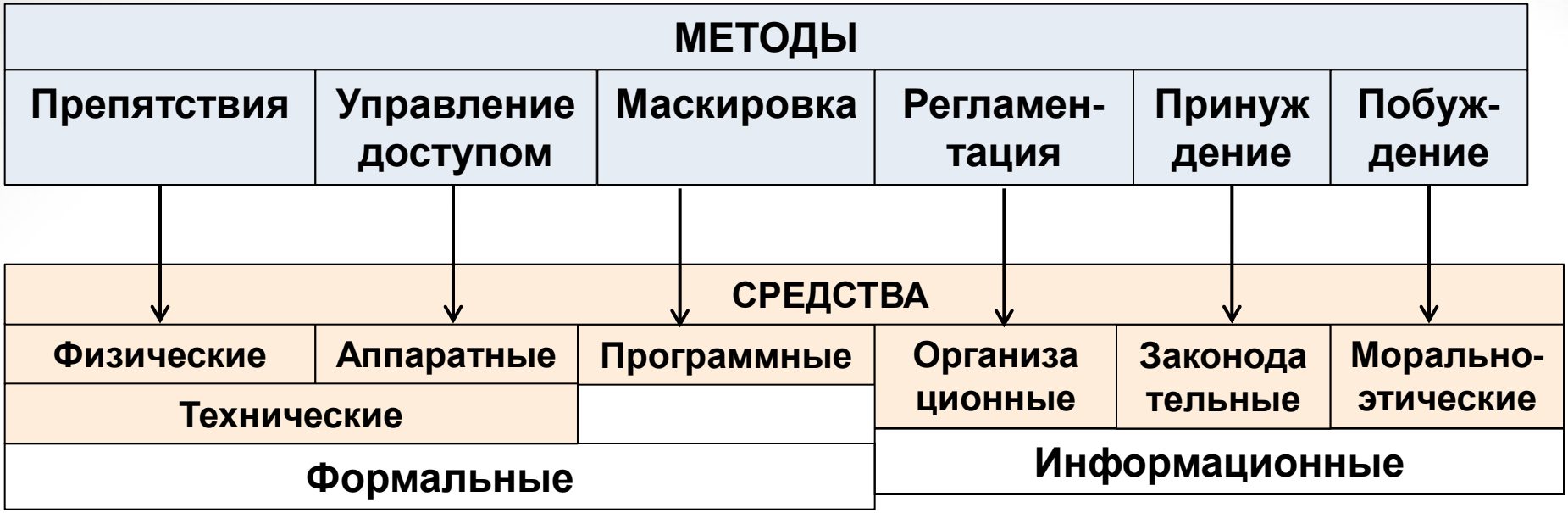
3. Методы и средства защиты информации

Проблема создания *системы защиты информации включает две взаимодополняющие задачи:*

1) разработка системы защиты информации (ее синтез);
2) оценка разработанной системы защиты информации.

Вторая задача решается путем анализа ее технических характеристик с целью установления, удовлетворяет ли система защиты, информации комплексу требований к данным системам. Такая задача в настоящее время решается почти исключительно экспертным путем с помощью сертификации средств защиты информации и аттестации системы защиты информации в процессе ее внедрения.

Методы и средства обеспечения безопасности информации в САПР



Препятствия — методы 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 в себя следующие ***функции защиты***:

- идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);
- 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;
- регистрацию (сигнализация, отключение, задержка работ, отказ в запросе) при попытках несанкционированных действий.

- ***Маскировка*** — метод защиты информации путем ее криптографического закрытия. Этот метод широко применяется как при обработке, так и при хранении информации, в том числе на мобильных носителях информации. При передаче информации по каналам связи большой протяженности данный 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*** — 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*** — метод защиты, который побуждает пользователя и персонал системы не нарушать установленный порядок за счет соблюдения сложившихся моральных и этических норм (как регламентированных, так и неписаных).

Основные средства защиты

1. *Технические средства*
2. *Физические средства*
3. *Программные средства*
4. *Организационные средства*
5. *Морально-этические средства*
6. *Законодательные средства*

Основным средством защиты от вирусов служит ***архивирование***.

Другие методы заменить его не могут, хотя и повышают общий уровень защиты. Архивирование необходимо делать ежедневно. Архивирование заключается в создании копий используемых файлов и систематическом обновлении изменяемых файлов.

В целях профилактики для защиты от вирусов рекомендуется:

- работа с флэш-картами, защищенными от записи;
- минимизация периодов доступности мобильных носителей информации (МНИ) для записи;
- разделение МНИ между конкретными ответственными пользователями;
- разделение передаваемых и поступающих МНИ;
- разделение хранения вновь полученных программ и эксплуатировавшихся ранее;
- проверка вновь полученного программного обеспечения на наличие в них вируса тестирующими программами;
- хранение программ на жестком диске в архивированном виде.

Чтобы избежать появления компьютерных вирусов

- не переписывать программное обеспечение с других компьютеров, если это необходимо, то следует принять перечисленные выше меры;
- не допускать к работе на компьютере посторонних лиц, особенно если они собираются работать со своими МНИ;
- не пользоваться посторонними МНИ, особенно с компьютерными играми.

Типичные ошибки пользователя

- отсутствие надлежащей системы архивации информации;
- запуск полученной программы без ее предварительной проверки на зараженность и без установки максимального режима защиты винчестера с помощью систем разграничения доступа и запуска резидентного сторожа;
- выполнение перезагрузки системы при наличии установленной в USB входе флэш-накопителя (при этом BIOS делает попытку загрузиться именно с этого накопителя, а не с винчестера; в результате, если флэшка заражена бутовым вирусом, происходит заражение винчестера);
- прогон всевозможных антивирусных программ, без знания типов диагностики одних и тех же вирусов разными антивирусными программами;
- анализ и восстановление программ на зараженной операционной системе.

Логотипы наиболее распространенных фирм производителей антивирусного ПО.

- Среди наиболее популярных у российских пользователей антивирусных пакетов назовем программы: Norton Antivirus, Антивирус Касперского, Dr.Web, и Secret Net Studio 8.1 («Код Безопасности»).
- Существуют программы-фильтры, проверяющие, имеется ли в файлах (на указанном пользователем диске) специальная для данного вируса комбинация байтов. Используется также специальная обработка файлов, дисков, каталогов — ***вакцинация***: запуск программ-вакцин, имитирующих сочетание условий, в которых начинает работать и проявляет себя данный тип вируса.

П А М Я Т К А
по обеспечению режима безопасности и эксплуатации оборудования, установленного в защищаемом помещении (Примерный текст)

1. Ответственность за режим безопасности в защищаемом помещении (ЗП) и правильность использования установленных в нем технических средств несет лицо, которое постоянно в нем работает, или лицо, специально на то уполномоченное.

2. Установка нового оборудования, мебели и т.п. или замена их, а также ремонт помещения должны проводиться только по согласованию с подразделением (специалистом) по защите информации предприятия.

3. В нерабочее время помещение должно закрываться на ключ.

4. В рабочее время, в случае ухода руководителя, помещение должно закрываться на ключ или оставляться под ответственность лиц назначенных руководителем подразделения.

5. При проведении конфиденциальных мероприятий бытовая радиоаппаратура, установленная в помещении (телевизоры, радиоприемники и т.п.), должна отключаться от сети электропитания.

П А М Я Т К А
по обеспечению режима безопасности и эксплуатации оборудования, установленного в защищаемом помещении (Примерный текст)

6. Должны выполняться предписания на эксплуатацию средств связи, вычислительной техники, оргтехники, бытовых приборов и др. оборудования, установленного в помещении.

7. Запрещается использование в ЗП радиотелефонов, оконечных устройств сотовой и транкинговой связи. При установке в ЗП телефонных и факсимильных аппаратов с автоответчиком, спикерфоном и имеющих выход в городскую АТС, следует отключать эти аппараты на время проведения конфиденциальных мероприятий.

8. Повседневный контроль за выполнением требований по защите помещения осуществляют лица, ответственные за помещение, и служба безопасности предприятия.

9. Периодический контроль эффективности мер защиты помещения осуществляется специалистами по защите информации.