ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ ИМЕНИ А.Ф. МОЖАЙСКОГО

Кафедра № 63 Математического и программного обеспечения

УТВЕРЖДАЮ
Начальник 63 кафедры
полковник_____С.Войцеховский

«___» _____ 2015 г.

Автор: преподаватель 63 кафедры
Кандидат технических наук
майор С.Краснов

Лекция № 2

Тема: «КЛАССИФИКАЦИЯ УГРОЗ И УЯЗВИМОСТЕЙ ИПО»

по дисциплине: «Защита информации»

Обсуждено и одобрено на заседании 63 кафедры
протокол № __ «____» _____ 2015 г.

Санкт-Петербург
2015

Содержание занятия и время

Введение – 5 мин.

Учебные вопросы (основная часть):

1. Основные определения – 20 мин.
2. Классификация источников угроз – 20 мин.
3. Классификация уязвимостей безопасности – 20 мин.

Виды угроз ИПО. Направления формализации процессов защиты информации. Матричные и многоуровневые модели доступа – 20 мин.

Заключение – 3-5 мин.

Литература:

Основная:

1. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 134 с.
2. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – 252 с.

Дополнительная:

1. Вихорев С.В. Классификация угроз информационной безопасности. - http://www2.cnews.ru/comments/security/elvis_class.shtml
2. Войцеховский С.В., Марковский А.С., Палагушин В.А. Защита информации в автоматизированных системах./ Под ред. профессора Хомоненко А.Д. – Спб.:НТЦ им. Л.Т. Тучкова, 2005. – 149 с.

Материально техническое обеспечение:

1. Технические средства обучения: ПЭВМ, мультимедиа проектор, экран, программное обеспечение.
2. Приложения (слайды).
3. Наглядные средства обучения – доска, мел.

Организационно-методические указания:

Цель лекции: *Дать знания в области классификации угроз и уязвимостей ИПО.*

Во введении сформулировать тему лекции, цель и название изучаемых вопросов. При этом произвести опрос курсантов по пройденному материалу.

Применяемым методическим приемом является рассказ.

В основной части сконцентрировать внимание курсантов на основных определениях предметной области ЗИ, классификации источников угроз и уязвимостей безопасности информации.

В заключительной части обобщить изложенный материал и осуществить контрольный опрос.

1. Дайте определение угрозы безопасности информации?
2. Дайте определение уязвимости информационной системы?
3. Дайте классификацию источников угроз информационной безопасности?
4. Дайте классификацию уязвимостей безопасности?

Отвечаю на вопросы по теме занятия, даю задание на самостоятельную подготовку – ознакомиться и законспектировать:

1. РД «Концепция защиты СВТ и АС от НСД к информации».
2. РД «Классификация СВТ по уровню защищенности от НСД».
3. РД «Классификация АС по уровню защищенности от НСД».

«Классификация угроз и уязвимостей ИПО»

В. 1. Основные определения.

Угроза безопасности информации представляет собой совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее [1].

Угрозы сами по себе не проявляются. Все угрозы могут быть реализованы (с помощью *методов реализации*) только при наличии каких-нибудь слабых мест – *уязвимостей,* присущих конкретной АС.

Уязвимость информационной системы – любая характеристика или элемент информационной системы, использование которых нарушителем может привести к реализации угрозы. [13]

Если есть какие-либо действия, то есть и носители этих действий, из которых эти угрозы могут исходить – ***источники угроз (ИУ).*** В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления.

Структура понятия «угрозы безопасности информации» представлена на рис. 2.

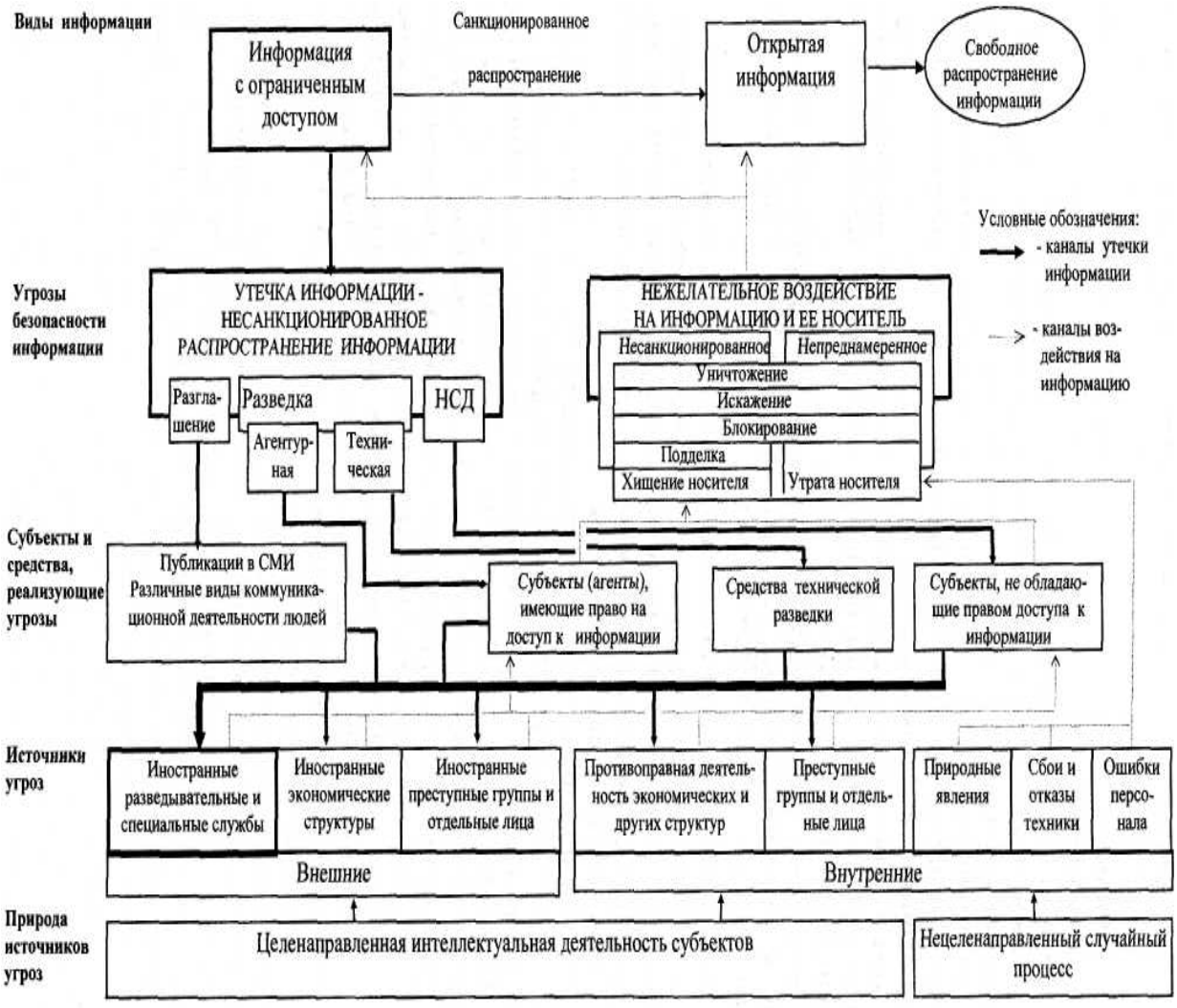


Рис. 2. Структура понятия "угрозы безопасности информации"

В. 2. Классификация источников угроз

Носителями угроз безопасности информации являются источники угроз. В качестве источников угроз могут выступать как субъекты (личность) так и объективные проявления. Причем, источники угроз могут находиться как внутри защищаемой организации - внутренние источники, так и вне ее - внешние источники. Деление источников на субъективные и объективные оправдано исходя из предыдущих рассуждений по поводу вины или риска ущерба информации. А деление на внутренние и внешние источники оправдано потому, что для одной и той же угрозы методы парирования для внешних и внутренних источников могу быть разными.

Все источники угроз безопасности информации можно разделить на три основные группы:

1. Обусловленные действиями субъекта (антропогенные источники угроз).
2. Обусловленные техническими средствами (техногенные источники угрозы).
3. Обусловленные стихийными источниками.

1. Антропогенные источники угроз

Антропогенными источниками угроз безопасности информации выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления. Только в этом случае можно говорит о причинении ущерба. Эта группа наиболее обширна и представляет наибольший интерес с точки зрения организации защиты, так как действия субъекта всегда можно оценить, спрогнозировать и принять адекватные меры. Методы противодействия в этом случае управляемы и напрямую зависят от воли организаторов защиты информации.

В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Субъекты (источники), действия которых могут привести к нарушению безопасности информации могут быть как внешние [I.A.], так и внутренние [I.B.].

Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним относятся:

1. [I.A.1] криминальные структуры;
2. [I.A.2] потенциальные преступники и хакеры;
3. [I.A.3] недобросовестные партнеры;
4. [I.A.4] технический персонал поставщиков телекоммуникационных услуг;
5. [I.A.5] представители надзорных организаций и аварийных служб;
6. [I.A.6] представители силовых структур.

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети. К ним относятся:

1. [I.B.1] основной персонал (пользователи, программисты, разработчики);
2. [I.B.2] представители службы защиты информации;
3. [I.B.3] вспомогательный персонал (уборщики, охрана);
4. [I.B.4] технический персонал (жизнеобеспечение, эксплуатация).

Необходимо учитывать также, что особую группу внутренних антропогенных источников составляют лица с нарушенной психикой и специально внедренные и завербованные агенты, которые могут быть из числа основного, вспомогательного и технического персонала, а также представителей службы защиты информации. Данная группа рассматривается в составе перечисленных выше источников угроз, но методы

парирования угрозам для этой группы могут иметь свои отличия. Квалификация антропогенных источников информации играют важную роль в оценке их влияния и учитывается при ранжировании источников угроз.

2. Техногенные источники угроз

Вторая группа содержит источники угроз, определяемые технократической деятельностью человека и развитием цивилизации. Однако, последствия, вызванные такой деятельностью вышли из под контроля человека и существуют сами по себе. Эти источники угроз менее прогнозируемые, напрямую зависят от свойств техники и поэтому требуют особого внимания. Данный класс источников угроз безопасности информации особенно актуален в современных условиях, так как в сложившихся условиях эксперты ожидают резкого роста числа техногенных катастроф, вызванных физическим и моральным устареванием технического парка используемого оборудования, а также отсутствием материальных средств на его обновление.

Технические средства, являющиеся источниками потенциальных угроз безопасности информации так же могут быть внешними [II.A.]:

1. [II.A.1] средства связи;
2. [II.A.2] сети инженерных коммуникации (водоснабжения, канализации);
3. [II.A.3] транспорт.

и внутренними [II.B.]:

1. [II.B.1] некачественные технические средства обработки информации;
2. [II.B.2] некачественные программные средства обработки информации;
3. [II.B.3] вспомогательные средства (охраны, сигнализации, телефонии);
4. [II.B.4] другие технические средства, применяемые в учреждении;

3. Стихийные источники угроз

Третья группа источников угроз объединяет, обстоятельства, составляющие непреодолимую силу, то есть такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. К непреодолимой силе[17] в законодательстве и договорной практике относят стихийные бедствия или иные обстоятельства, которые невозможно предусмотреть или предотвратить или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей. Такие источники угроз совершенно не поддаются прогнозированию и поэтому меры защиты от них должны применяться всегда.

Стихийные источники потенциальных угроз информационной безопасности как правило являются внешними по отношению к защищаемому объекту и под ними понимаются прежде всего природные катаклизмы [III.A.]:

1. [III.A.1] пожары;
2. [III.A.2] землетрясения;
3. [III.A.3] наводнения;
4. [III.A.4] ураганы;
5. [III.A.5] различные непредвиденные обстоятельства;
6. [III.A.6] необъяснимые явления;
7. [III.A.7] другие форс-мажорные обстоятельства, то есть различные решения высших государственных органов, забастовки, войны, революции и т. п., приводящие к возникновению обстоятельств непреодолимой силы.

B. 3. Классификация уязвимостей безопасности

Угрозы, как возможные опасности совершения какого-либо действия, направленного против объекта защиты, проявляются не сами по себе, а через уязвимости, приводящие к нарушению безопасности информации на конкретном объекте информатизации.

Уязвимости присущи объекту информатизации, неотделимы от него и обуславливаются недостатками процесса функционирования, свойствами архитектуры автоматизированных систем, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации и расположения. Источники угроз могут использовать уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу, пользователю информации) Кроме того, возможно не злонамеренные действия источников угроз по активизации тех или иных уязвимостей, наносящих вред.

Каждой угрозе могут быть сопоставлены различные уязвимости. Устранение или существенное ослабление уязвимостей влияет на возможность реализации угроз безопасности информации.

Для удобства анализа, уязвимости разделены на классы (обозначаются заглавными буквами), группы (обозначаются римскими цифрами) и подгруппы (обозначаются строчными буквами). Уязвимости безопасности информации могут быть:

1. [A] объективными
2. [B] субъективными
3. [C] случайными.

1. Объективные уязвимости зависят от особенностей построения и технических характеристик оборудования, применяемого на защищаемом объекте. Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно-техническими методами защиты информации. К ним можно отнести:

[**A.I**] ***сопутствующие техническим средствам излучения***

- *[A.I.a] электромагнитные (побочные излучения элементов технических средств, кабельных линий технических средств, излучения на частотах работы генераторов, на частотах самовозбуждения усилителей)*
- [A.I.b] электрические (наводки электромагнитных излучений на линии и проводники, просачивание сигналов в цепи электропитания, в цепи заземления, неравномерность потребления тока электропитания)
- [A.I.c] звуковые (акустические, виброакустические)

[**A.II**] ***активизируемые***

- [A.II.a] аппаратные закладки (устанавливаемые в телефонные линии, в сети электропитания, в помещениях, в технических средствах)
- [A.II.b] программные закладки (вредоносные программы, технологические выходы из программ, нелегальные копии ПО)

[**A.III**] ***определяемые особенностями элементов***

- *[A.III.a] элементы, обладающие электроакустическими преобразованиями (телефонные аппараты, громкоговорители и микрофоны, катушки индуктивности, дроссели, трансформаторы и пр.)*
- [A.III.b] элементы, подверженные воздействию электромагнитного поля (магнитные носители, микросхемы, нелинейные элементы, поверженные ВЧ навязыванию)

[A.IV] ***определяемые особенностями защищаемого объекта***

- [A.IV.a] местоположением объекта (отсутствие контролируемой зоны, наличие прямой видимости объектов, удаленных и мобильных элементов объекта, вибрирующих отражающих поверхностей)
- [A.IV.b] организацией каналов обмена информацией (использование радиоканалов, глобальных информационных сетей, арендуемых каналов)

2. Субъективные уязвимости зависят от действий сотрудников и, в основном, устраняются организационными и программно-аппаратными методами:

[B.I] ***ошибки***

- [B.I.a] при подготовке и использовании программного обеспечения (при разработке алгоритмов и программного обеспечения, инсталляции и загрузке программного обеспечения, эксплуатации программного обеспечения, вводе данных)
- [B.I.b] при управлении сложными системами (при использовании возможностей самообучения систем, настройке сервисов универсальных систем, организации управления потоками обмена информации)
- [B.I.c] при эксплуатации технических средств (при включении/выключении технических средств, использовании технических средств охраны, использовании средств обмена информацией)

[B.II] ***нарушения***

- [B.II.a] режима охраны и защиты (доступа на объект, доступа к техническим средствам)
- [B.II.b] режима эксплуатации технических средств (энергообеспечения, жизнеобеспечения)
- [B.II.c] режима использования информации (обработки и обмена информацией, хранения и уничтожения носителей информации, уничтожения производственных отходов и брака)
- [B.II.d] режима конфиденциальности (сотрудниками в нерабочее время, уволенными сотрудниками).

3. Случайные уязвимости зависят от особенностей окружающей защищаемый объект среды и непредвиденных обстоятельств. Эти факторы, как правило, мало предсказуемы и их устранение возможно только при проведении комплекса организационных и инженерно-технических мероприятий по противодействию угрозам информационной безопасности:

[C.I] ***сбои и отказы***

- [C.I.a] отказы и неисправности технических средств (обрабатывающих информацию, обеспечивающих работоспособность средств обработки информации, обеспечивающих охрану и контроль доступа)
- [C.I.b] старение и размагничивание носителей информации (дискет и съемных носителей, жестких дисков, элементов микросхем, кабелей и соединительных линий)
- [C.I.c] сбои программного обеспечения (операционных систем и СУБД, прикладных программ, сервисных программ, антивирусных программ)
- [C.I.d] сбои электроснабжения (оборудования, обрабатывающего информацию, обеспечивающего и вспомогательного оборудования)

[C.II] ***повреждения***

- [C.II.a] жизнеобеспечивающих коммуникаций (электро-, водо-, газо-, теплоснабжения, канализации, кондиционирования и вентиляции)
- [C.II.b] ограждающих конструкций (внешних ограждений территорий, стен и перекрытий зданий [1], корпусов технологического оборудования)

В. 4. Виды угроз ИПО.

Угрозы безопасности ИПО, от которых необходимо обеспечить защиту объектов, *включают* **утечку** информации, составляющую тайну вследствие использования нарушителем имеющихся уязвимостей (каналов утечки) **и нежелательные воздействия** на информацию и/или ее носитель исходящие из ИУ.

Возникновение и реализация угроз безопасности информации происходят при:

- возникновении условий, порождающих источники угроз безопасности информации;
- появлении потенциальных источников угроз;

- появлении реальных источников угроз (трансформация потенциальных источников угроз в реальные угрозы);
- возникновении факторов, способствующих реализации угрозы утечки информации, несанкционированных и/или непреднамеренных воздействий на информацию;
- реализации угрозы, т. е. наступлении события, заключающегося в утечке информации, несанкционированном и/или непреднамеренном воздействии на информацию;
- нанесении ущерба объекту защиты и/или другим объектам вследствие утечки информации, несанкционированных и/или непреднамеренных воздействий на информацию.

Таким образом, **угроза** реализуется в виде цепочки или сети условий и факторов (частных угроз) и их последствий. Возникшие последствия реализации частной угрозы, в свою очередь, также могут становиться угрозой, содержащей условия и факторы для возникновения более отдаленных негативных последствий.

Утечка информации может происходить по различным каналам в результате ее разглашения, добывания информации агентурной и технической разведками, несанкционированного доступа к информации.

Нежелательные воздействия на информацию и/или ее носитель подразделяются на воздействия несанкционированные (преднамеренные) и непреднамеренные, которые могут приводить к уничтожению, искажению, блокированию, подделке информации, хищению или утрате ее носителя. Защите от этих воздействий подлежит как информация, составляющая тайну, так и открытая информация. Угрозы утечки информации могут реализовываться субъектами, имеющими право на доступ к информации и не обладающими таким правом.

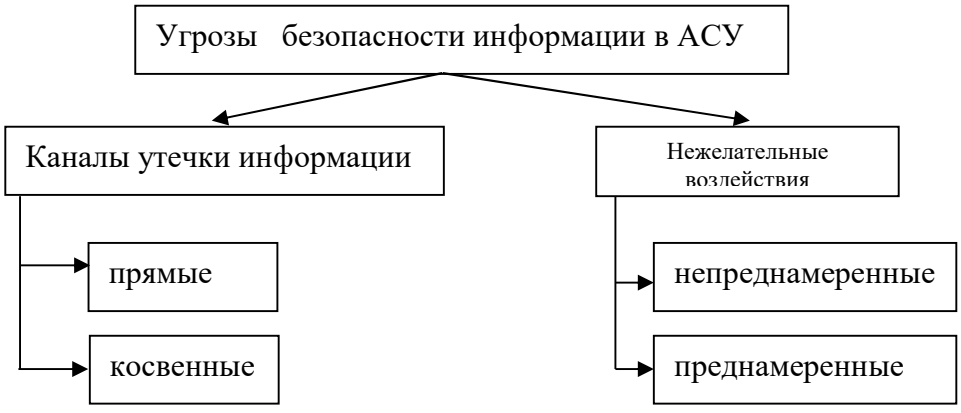
Нарушение безопасности данных в АСУ возможно как вследствие использования нарушителем каналов утечки данных, так и вследствие различных воздействий, в результате которых происходит уничтожение (модификация) данных или создаются каналы утечки данных (рис. 3.1).

Под каналом утечки данных в рассматриваемом случае будем понимать потенциальную возможность такого доступа к данным, которая обусловлена архитектурой к технологической схемой функционирования АСУ, а также существующей организацией работы с данными.

Все каналы утечки данных в АСУ можно разделить на косвенные и прямые.

Косвенными называется такие каналы утечки данных, использование которых для НСД не требует непосредственного доступа к данным и техническим устройствам АСУ. *Косвенные каналы утечки данных возникают вследствие:*

- недостаточной звукоизоляции и светозащищенности помещений;
- недостаточной защищенности технических средств АСУ от электромагнитных излучений;
- просчетов в организации применения морально-этических, законодательных и организационных методов и средств защиты информации.



Прямые каналы утечки данных требуют непосредственного доступа к данным и техническим средствам АСУ и, в свою очередь, подразделяются на каналы утечки с модификацией данных и без модификации данных.

Наличие прямых каналов утечки данных обусловлено недостаточной защищенностью технических и программных средств АСУ, недостатками ОС, СУБД, языков программирования и другого математического обеспечения, а также просчетами в организации процесса работы с данными, недостатками законодательства и др.

Косвенные каналы утечки данных могут быть использованы нарушителем, если имеют место следующие стратегии:

- применение подслушивающих устройств;
- применение дистанционного фотографирования;
- перехват электромагнитных излучений;
- хищение носителей данных;
- хищение производственных отходов (перфолент, перфокарт, распечаток программ и т.д.).

Прямые каналы утечки данных позволяют нарушителю несанкционированно подключиться к аппаратуре и выполнить действия по анализу и модификации хранимых, обрабатываемых и передаваемых данных. Для воздействия на данные, а также в целях организации нормальной работы сети нарушитель может осуществить следующие действия:

- получить доступ к терминалу;
- работать за пользователя АСУ;
- подменить пользователя;
- подобрать пароль.

Нежелательные воздействия на АСУ можно подразделить на *преднамеренные (несанкционированные) и непреднамеренные.* Анализ опыта проектирования, изготовления и эксплуатации АСУ показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни и функционирования АСУ. Причинами непреднамеренных воздействий при эксплуатации АСУ могут быть:

• аварийные ситуации из-за стихийных бедствий и отключений электропитания;
• отказы и сбои аппаратуры;
• ошибки в программном обеспечении;
• ошибки в работе обслуживающего персонала и пользователей;
• помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия связаны с целенаправленными действиями нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник и т.д. Действия нарушителя могут быть обусловлены следующими мотивами:

- недовольством служащего своей карьерой;
- сугубо материальным интересом;
- любопытством;
- конкурентной борьбой;
- шпионажем;
- стремлением самоутвердиться любой ценой и т.п.

По цели воздействия различают три основных типа угроз безопасности АСУ:

- угрозы нарушения конфиденциальности информации;
- угрозы нарушения целостности информации;
- угрозы нарушения работоспособности системы (отказы в обслуживании).

Угрозы нарушения конфиденциальности направлены на разглашение конфиденциальной или секретной информации.

- хищение (копирование) информации и средств её обработки;

- утрата (неумышленная потеря, утечка) информации.

При реализации этих угроз информация становится известной лицам, которые не должны иметь к ней доступ. В терминах компьютерной безопасности угроза нарушения конфиденциальности имеет место всякий раз, когда получен несанкционированный доступ к некоторой закрытой информации, хранящейся в компьютерной системе |ли передаваемой от одной системы к другой.

Угрозы нарушения целостности информации, хранящейся компьютерной системе или передаваемой по каналу связи, направлены на ее изменение или искажение, приводящее к нарушению ее качества или полному уничтожению.

- модификация (искажение) информации;
- отрицание подлинности информации;
- навязывание ложной информации.

Целостность информации может быть нарушена умышленно злоумышленником, а также в результате объективных воздействий со стороны среды, окружающей систему. Эта угроза особенно актуальна для систем передачи информации - компьютерных сетей и систем телекоммуникаций. Умышленные нарушения целостности информации не следует путать с ее санкционированным изменением, которое выполняется полномочными лицами с обоснованной целью (например, таким изменением является периодическая коррекция некоторой базы данных).

Угрозы нарушения работоспособности (отказ в обслуживании) направлены на создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность АСУ, либо блокируют доступ к некоторым ее ресурсам.

- блокирование информации;
- уничтожение информации и средств её обработки.

Например, если один пользователь системы запрашивает доступ к некоторой службе, а другой предпринимает действия по блокированию этого доступа, то первый пользователь получает отказ в обслуживании. Блокирование доступа к ресурсу может быть постоянным или временным.

Нарушения конфиденциальности и целостности информации, а также доступности и целостности определенных компонентов и ресурсов АСУ могут быть вызваны различными опасными воздействиями на АСУ.

По месту возникновения угрозы можно охарактеризовать следующим образом: рис3.2.

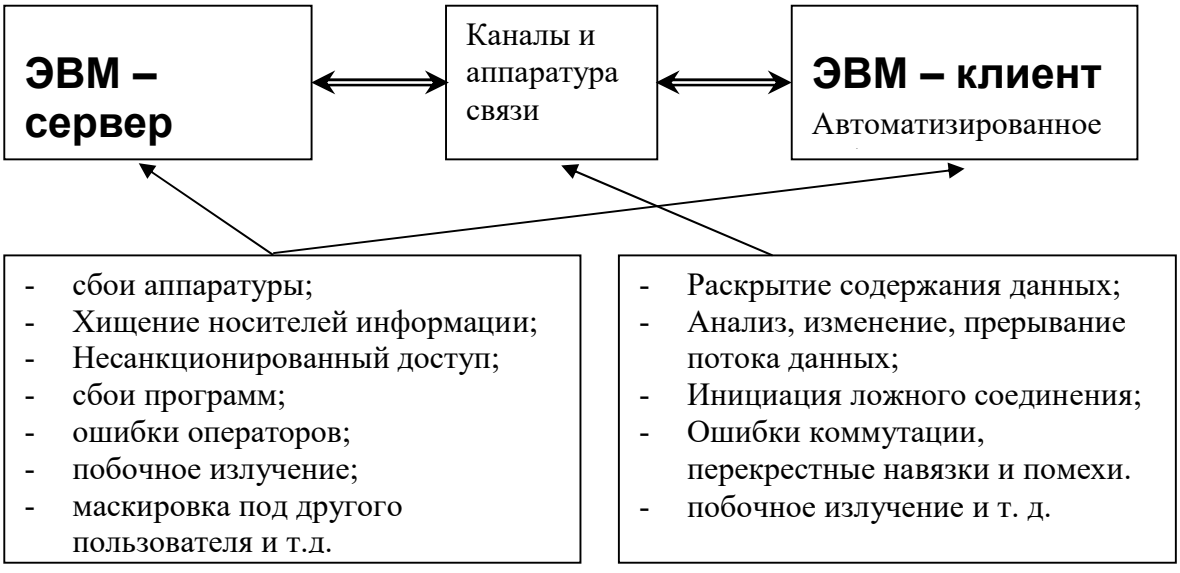


Рис.3.2

Современная автоматизированная система обработки информации представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными.

Моделирование процессов нарушения ИБ может осуществляться на основе рассмотрения логической цепочки: угроза – источник угрозы – метод реализации – уязвимость – последствия.

Основными *факторами, способствующими повышению уязвимости* АС являются:

- постоянное увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью АС;
- возрастание степени автоматизации обработки данных в АС;
- интеграция в единых базах данных информации больших объемов, различного назначения и различной принадлежности;
- усложнение режимов функционирования технических средств АС и увеличивающаяся сложность программного обеспечения;
- долговременное хранение данных на внешних носителях информации;
- постоянное расширение круга пользователей, имеющих доступ к ресурсам АС;
- возрастающая важность и ответственность решений, принимаемых на основе автоматизированной обработки данных в АС;
- большая концентрация и широкая территориальная расположенность АС;
- повышение интенсивности циркуляции информации между АС, объединенными в сети, расположенными друг от друга как на малом, так и на большом расстоянии.

Эти и другие факторы позволяют сделать вывод, что по мере развития средств вычислительной техники, уязвимость АС постоянно возрастает.
В связи с этим проблема защиты информационно – программного обеспечения автоматизированных систем стала одной из главных проблем в области автоматизированной обработки данных.

В. 5. Направления формализации процессов защиты информации, матричные и многоуровневые модели доступа

В настоящее время известно большое количество работ по формализации процессов обеспечения безопасности информации. Многообразие разработанных формальных моделей безопасности ставит вопрос об анализе существующих моделей при проектировании систем защиты. Представленные формальные модели безопасности отличаются следующим: они разработаны в разное время; рассматривают проблему защиты информации под различными углами и в своих технических условиях обеспечивают различные уровни детализации.

Поскольку отразить в виде формальной модели всю сложность реальной обстановки трудно, то любая модель по некоторым аспектам отличается от идеальной. Обычно формальные модели безопасности описывают средства защиты информации с более жесткими характеристиками, чем у средств защиты, используемых в реальной среде; любые операции, которые подчиняются структурам модели, будут безопасными согласно стандартным определениям, а некоторые операции, не принимаемые моделью, будут, тем не менее, считаться безопасными вне формальной модели безопасности. При этом использование для повышения безопасности сильно ограничивающих формальных моделей может привести к созданию систем, неприемлемых для предполагаемых условий реализации.

Напомним, что под политикой безопасности понимается совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от определенного множества угроз и составляет необходимое (а иногда и достаточное) условие безопасности системы. Формальное выражение политики безопасности называют моделью политики безопасности.

Для чего же нужны модели безопасности? Неужели нельзя обойтись неформальным описанием политики безопасности, ведь составление формальных моделей требует существенных затрат и привлечения высококвалифицированных специалистов, они трудны для понимания и требуют определенной интерпретации для применения в реальных системах. Тем не менее формальные модели необходимы и используются достаточно широко, потому что только с их помощью можно доказать безопасность системы опираясь при этом на объективные и неопровержимые постулаты математической теории. По своему назначению модели безопасности аналогичны аэродинамическим моделям самолетов и моделям плавучести кораблей — и те, и другие позволяют обосновать жизнеспособность системы и определяют базовые принципы ее архитектуры и используемые при ее построении технологические решения. Основная цель создания политики безопасности информационной системы и описания ее в виде формальной модели — это определение условий, которым должно подчиняться поведение системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений. На практике это означает, что только соответствующим образом уполномоченные пользователи получат доступ к информации, и смогут осуществлять с ней только санкционированные действия.

Кроме того, формальные модели безопасности позволяют решить еще целый ряд задач, возникающих в ходе проектирования, разработки и сертификации защищенных систем, поэтому их используют не только теоретики информационной безопасности, но и другие категории специалистов, участвующих в процессе создания и эксплуатации защищенных информационных систем (производители, потребители, эксперты-квалификаторы).

Производители защищенных информационных систем используют модели безопасности в следующих случаях:

1. *при составлении формальной спецификации политики безопасности разрабатываемой системы;*
2. при выборе и обосновании базовых принципов архитектуры защищенной системы, определяющих механизмы реализации средств защиты;
3. *в процессе анализа безопасности системы в качестве эталонной модели;*
4. *при подтверждении свойств разрабатываемой системы путем формального доказательства соблюдения политики безопасности.*

Потребители путем составления формальных моделей безопасности получают возможности довести до сведения производителей свои требования в четко определенной и непротиворечивой форме, а также оценить соответствие защищенных систем своим потребностям.

Эксперты по квалификации в ходе анализа адекватности реализации политики безопасности в защищенных системах используют модели безопасности в качестве эталонов.

В данном разделе изложены основные положения наиболее распространенных политик безопасности, основанных на контроле доступа субъектов к объектам, и моделирующих поведение системы с помощью пространства состояний, одни из которых являются безопасными, а другие — нет. Все **рассматриваемые *модели безопасности* основаны на следующих *базовых представлениях***:

1. Система является совокупностью взаимодействующих сущностей — *субъектов* и *объектов. Объекты* можно интуитивно представлять в виде контейнеров, содержащих информацию, а *субъектами* считать выполняющиеся программы, которые воздействуют на *объекты* различными способами. При таком представлении системы безопасность обработки информации обеспечивается путем решения задачи управления доступом

субъектов к *объектам* в соответствии с заданным набором правил и ограничений, которые образуют политику безопасности. Считается, что система безопасна, если субъекты не имеют возможности нарушить правила политики безопасности. Необходимо отметить, что общим подходом для всех моделей является именно разделение множества сущностей, составляющих систему, на множества субъектов и объектов, хотя сами определения понятий *объект* и *субъект* в разных моделях могут существенно различаться.

2. Все взаимодействия в системе моделируются установлением отношений определенного типа между субъектами и объектами. Множество типов отношений определяется в виде набора операций, которые субъекты могут производить над объектами.

3. Все операции контролируются монитором взаимодействий и либо запрещаются, либо разрешаются в соответствии с правилами политики безопасности.

4. Политика безопасности задается в виде правил, в соответствии с которыми должны осуществляться все взаимодействия между субъектами и объектами. Взаимодействия, приводящие к нарушению этих правил, пресекаются средствами контроля доступа и не могут быть осуществлены.

5. Совокупность множеств субъектов, объектов и отношений между ними (установившихся взаимодействий) определяет *состояние* системы. Каждое состояние системы является либо *безопасным,* либо *небезопасным* в соответствии с предложенным в модели критерием безопасности.

6. Основной элемент модели безопасности — это доказательство утверждения (теоремы) о том, что система, находящаяся в безопасном состоянии, не может перейти в небезопасное состояние при соблюдении всех установленных правил и ограничений.

Матричные и многоуровневые модели доступа

Метод управления доступом опирается на выбранную модель доступа. В настоящее время наибольшее распространение получили матричные и многоуровневые модели доступа. Указанным моделям соответствуют дискретное (избирательное) и мандатное управление доступом.

Рассмотрим так называемую **матричную модель** защиты, получившую на сегодняшний день широкое распространение. В её основе лежит **модель Харрисона-Руззо-Ульмана.**

При использовании матричной модели доступа условия доступа каждого субъекта 's' к каждому объекту 'o' определяются содержимым элемента матрицы доступа или матрицы установления полномочий M.

Каждый элемент M_{ij} матрицы доступа M определяет права доступа i-го субъекта к j-му объекту (читать, писать, выполнять, нельзя использовать и т.п.). Пример матрицы доступа приведен в Таблице 1.

Элементы в матрице доступа, приведенные в Таблице 1, имеют следующие значения: r- чтение, w- запись, x- выполнение.

Таблица 1

Субъекты	Объекты		
	O1	02	On
S1	r	w	w
S2	rw	rw	-
…			
Sm	x	xrw	xw

Элементы матрицы доступа могут содержать указатели на специальные процедуры, которые должны выполняться при обращении субъекта к объекту. Решение о доступе в этом случае осуществляется на основании результатов выполнения процедур, например:

- решение о доступе в данный момент времени основывается на анализе предыдущих доступов к другим объектам;
- решение о доступе основывается на динамике состояния системы (права доступа субъекта зависят от текущих прав доступа других субъектов);
- решение о доступе основывается на значении определенных переменных, например, на значении таймера.

Отметим, что строка M[s,*] содержит список разрешенных операций субъекта V по отношению ко всем объектам (список возможностей), а столбец M[*,o] -определяет, какие субъекты имеют права доступа к объекту "o" и какие именно права доступа (список доступа).

Размерность матрицы доступа зависит от количества субъектов и объектов в системе и может быть достаточно большой. Для уменьшения размерности матрицы доступа применяются различные методы:

- установление групп субъектов, называемых кликами, каждая из которых представляет собой группу субъектов с одинаковыми правами;
- установление групп терминалов по классам полномочий (клики терминалов);
- группировка объектов по уровням категорий (например, по уровням секретности);
- хранение списка пар вида (o,f), где o - защищаемый объект, а f -разрешение на использование его субъектом.

Перечисленные методы и другие, им подобные, Применяются как по отдельности, так и в совокупности.

В процессе функционирования системы множества субъектов и объектов могут динамически изменяться. Такие изменения могут происходить, например, в результате появления новых субъектов и объектов, уничтожения субъектов и объектов и изменения прав доступа субъектов к объектам. Соответственно, в процессе функционирования системы должна изменяться и матрица доступа.

Матрицы доступа в той или иной степени используются во многих защищенных системах. С помощью матрицы доступа может быть описано состояние любой, сколь угодно сложной системы защиты в произвольный момент ее существования. Однако, несмотря на гибкие изобразительные возможности, **матричным моделям присущи и серьезные недостатки**.

Во-первых, низкий, излишне детализированный уровень описания отношений субъектов и объектов затрудняет анализ соблюдения так называемых правил разграничения доступа, то есть тех высокоуровневых отношений между субъектами - людьми и объектами - документами, которые приняты в социальных группах для регулирования доступа к секретным и другим охраняемым данным.

Во-вторых, вследствие трудно поддающегося регулированию разрастания размеров матриц доступа в реальных системах, процедуры по их обслуживанию и поддержанию в адекватном изменяемым условиям состоянии, оказываются весьма трудоемкими. Централизованная в руках администратора защиты служба сопровождения становится узким местом в работе систем, обладающих динамикой состава пользователей и программ.

Для преодоления указанных выше недостатков матричных моделей разработаны так называемые многоуровневые модели защиты, классическими примерами которых являются **модель** *конечных состояний* **Белла и Лападулы** и *решетчатая* **модель Деннинга.**

Многоуровневые модели переносят в операционную среду ЭВМ, и мир "электронных" документов, общепринятые и хорошо отработанные принципы обращения

с бумажными секретами, конфиденциальными документами, в течение многих лет применяемые на практике.

Многоуровневая модель является системой (не дискреционного) мандатного управления доступом. Ресурсам многоуровневой модели приписываются степени секретности, а субъектам - степени допуска. Наличие или отсутствие разрешения доступа субъекта к ресурсу является функцией степени допуска данного субъекта и степени секретности данного ресурса.

Разделение по уровням секретности опирается на теорию алгебраических решеток. Данные могут передаваться между ресурсами, если удовлетворяются следующие аксиомы (здесь буквами **a, b** и **c** будем обозначать идентификаторы ресурсов, а буквами **x, y, z** - их уровни секретности):

1) данные могут передаваться ресурсом самому себе;

2) данные могут передаваться от ресурса **a** к ресурсу **c,**, если они могут передаваться от ресурса **a** к ресурсу **b**, а от ресурса **b** к ресурсу **c** , т.е. если **x≤y** и **y≤z**, то **x≤z**;

3) если справедливы неравенства, **x≤y** и **y≤x** то **x=y**.

Рассмотренные аксиомы алгебраической решетки могут быть использованы для построения многоуровневой модели доступа.

Активные элементы вычислительного процесса (пользователи, задачи и т.п.) при многоуровневой защите наделяются определенными правами доступа, надежно зафиксированными в мандате субъекта. Для задачи (процесса) они, например, могут определятся в соответствии с уровнем допуска лица, обслуживаемого данной задачей. Пассивные элементы вычислительного процесса - разнообразные контейнеры данных (периферийные устройства внешней памяти, тома и наборы данных, файлы, разделы, сегменты внешней и основной памяти т.п.) наделяются определенными признаками конфиденциальности, зависящими от уровня содержащейся в этих контейнерах информации.

Признаки конфиденциальности надежно фиксируются в метке объекта. (В связи с использованием терминов "мандат" и "метка" многоуровневую защиту часто называют мандатной защитой или защитой с метками конфиденциальности). Права доступа каждого субъекта и характеристики конфиденциальности каждого объекта отображаются в виде совокупности уровня конфиденциальности и набора категорий конфиденциальности (возможно пустого). Уровень конфиденциальности может принимать одно из строго упорядоченного ряда фиксированных значений, например: конфиденциально, секретно, только для узкого круга лиц, несекретно и т.п.

Внутри отдельных уровней секретности для выделения разделов данных, требующих специального разрешения на доступ к ним, определены категории: стратегические, военно-морские и другие. Для получения доступа к данным определенной категории субъект должен иметь не только доступ к данным соответствующего уровня (по секретности), но и разрешение на доступ по категории. Например, субъект, имеющий доступ к данным с уровнем "совершенно секретно" и категории "стратегические", не может получить доступ к данным с категориями "военно-морские" уровня "совершенно секретно".

Рассмотрим **многоуровневую модель доступа, основанную на теории алгебраических решеток.** В системе защиты информации задается решетка ценностей. Все объекты (информация) отображаются в точки решетки. Объекты в многоуровневой модели имеют различные уровни доступа, а субъекты - степени допуска. Разрешение доступа субъекта к объекту является функцией от степени допуска конкретного субъекта и уровня доступа конкретного объекта. Схема модели системы защиты информации приведена на рис.1.

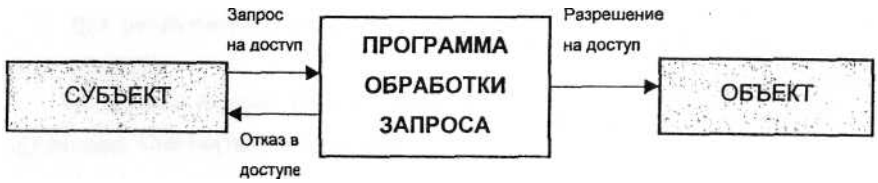


Рис.1

Для модели системы защиты информации определены следующие элементы:

S - множество субъектов;

O - множество объектов, не являющихся субъектами;

R - множество прав доступа.

R = {r,w,x,a},

Где: r - чтение объекта субъектом (получение субъектом данных, содержащихся в объекте);

w - запись-модификация данных объекта после их предварительного прочтения;

x - исполнение субъектом объекта (действие не связанное ни с чтением, ни с модификацией данных);

a - модификация данных объекта субъектом без их предварительного прочтения.

L - множество уровней доступа, обладающее свойством алгебраической решетки. Решетка строится как прямое произведение линейной решетки N и решетки SO подмножеств множества K. Элемент решетки SO имеет вид (n,k), где $n \in N, k \in SO$. Тогда для двух элементов решетки L:

$(n,k) < (n_1,k_1) \Leftrightarrow n < n_1, k \subseteq k_1.$

Линейный порядок N указывает гриф секретности. Элементы множества K - категории информации. Все объекты системы отображаются в точки {(n,k)} решетки L. M - матрица разрешенных доступов, $M = |M_{ij}|, M_{ij} \subseteq R$, i - номер субъекта, **j** - номер объекта. Матрица не содержит пустых столбцов. Q - множество запросов в систему. D - множество решений по запросам. D = {да, нет, ошибка}. B - множество текущих доступов.

$B \subseteq S \times O \times R$

$b \in B$ -данные вида (Sj,Oj,P), где

$S_i \in S,$

$O_j \in O,$

$P \in R.$

Для любого $(S,O,P) : P \in M_{so}$, где $M = |M_{so}|$ - матрица доступа на текущий момент времени.

F - подмножество множества $L^s \times L^s \times L^o$, где каждый элемент $f = (f_s,f_o,f_c), f \in F$ - вектор, который состоит из трех компонент, каждый из которых отображение:

f_s: S --> L - уровень допуска субъекта,

f_0: O --> L - уровень доступа объекта,

f_c: S --> L - текущий уровень доступа субъекта, зависящий от уровней доступа тех объектов, к которым субъект S имеет доступ в настоящий момент времени.

Для любого $S \in S, f_s(S) \geq f_c(S).$

H - текущий уровень иерархии объектов.

Множество $V = B \times M \times F \times H$ -множество состояний системы.

Множество $W \subseteq Q \times D \times V \times V$ - множество действий системы.

W = {(q,d,v_1,v_2)}, где

$q \in Q$ -поступивший в систему запрос,

$d \in D$ - принятое системой решение,

$v_1 \in V$ - система находилась в этом состоянии на момент запроса,

$v_2 \in V$ - система перешла в это состояние после выполнения принятого системой решения.

Вводится множество функций X, Y, Z:

$x : T \to Q$,

$y : T \to D$,

$z : T \to V$,

где T - множество значений времени (предполагаем, что время дискретно). Система Σ в модели системы защиты информации определена как подмножество X xY x Z .

$(x,y,z) \in \Sigma \Leftrightarrow (x_t, y_t, z_t, z_{t-1}) \in W$

Для любого t ***** T. Начальное состояние системы - zo**.

Для реализованной модели системы защиты информации определены два условия защиты:

1) простое условие защиты, служит для исключения прямой утечки секретной информации. Оно состоит в следующем. Если субъекту Sj запрещен доступ к объекту Oj:

по чтению - тогда $f_s(Si) < f_o(Oj)$; по записи - тогда $f_s(Si) < f_o(Oj)$.

2) '*' - условие защиты, предложено для предотвращения косвенной утечки секретной информации. Введение '*' - условия предназначено для исключения потоков данных вида «чтение объекта для перезаписи в объект с меньшим уровнем доступа». Это условие накладывает ограничения на уровни доступа тех объектов, к которым субъект может иметь доступ одновременно. Оно заключается в следующем. Если субъекту Si разрешен доступ к объекту OJ:

по чтению - тогда $f_c(Si) > f_o(Oj)$; по записи - тогда $f_c(Si) = f_o(Oj)$; по добавлению - тогда $\mathbf{f_0(Oj)} > f_c(Si)$.

Состояние системы считается безопасным, если соотношения между уровнями доступа объектов и допуска субъектов удовлетворяют как простому условию защиты, так и '*' - условию. То есть каждый текущий доступ $(S,O,P) \in B$ удовлетворяет простому условию защиты и '*'- условию.

Для обеспечения безопасности информации необходимо и достаточно, чтобы изменения состояний системы приводило только к безопасным состояниям, если исходное состояние было безопасным.

Поэтому модель системы защиты информации имеет строгие правила принятия решений по всем видам запросов, так чтобы действие системы приводило только к безопасным состояниям.

Классическая мандатная модель разработанная **Беллом и Лападулой** – *модель Белла-ЛаПадулы*

В мандатных моделях функция уровня безопасности F вместе с решеткой уровней определяют все допустимые отношения доступа между сущностями системы, поэтому множество состояний системы V представляется в виде набора упорядоченных пар (F,M), где M - это матрица доступа, отражающая текущую ситуацию с правами доступа субъектов к объектам, содержание которой аналогично матрице прав доступа в модели Харрисона-Руззо-Ульмана, но набор прав ограничен правами read и

write. Модель системы $\Sigma(v_0,R,T)$ состоит из начального состояния v_0, множества запросов R и функции перехода $T:(V\times R)\to V$, которая в ходе выполнения запроса переводит систему из одного состояния в другое. Система, находящаяся в состоянии $v\in V$, при получении запроса $r\in R$, переходит в следующее состояние $v^* = T(v,r)$. Состояние v достижимо в системе $\Sigma(v_0,R,T)$ тогда и только тогда, когда существует последовательность

$<(r_0,v_0),\ldots,(r_{n-1},v_{n-1}),(r_n,v)>$ такая, что $T(r_i, v_i) = v_{i+1}$ для $0\le i<n$.

Заметим, что для любой системы v_0 тривиально достижимо.

Как и для дискреционной модели состояния системы делятся на безопасные, в которых отношения доступа не противоречат установленным в модели правилам, и небезопасные, в которых эти правила нарушаются и происходит утечка информации.

Белл и ЛаПадула предложили следующее определение безопасного состояния:

1. Состояние (F,M) называется безопасным по чтению (или *просто безопасным)* тогда и только тогда, когда для каждого субъекта, осуществляющего в этом состоянии доступ чтения к объекту, уровень безопасности этого субъекта доминирует над уровнем безопасности этого объекта:

$\forall s\in S, \forall o\in O, read\in M[s,o]\to F(s)\ge F(o)$.

2. Состояние (F,M) называется безопасным по записи(или *-*безопасным*) тогда и только тогда, когда для каждого субъекта, осуществляющего в этом состоянии доступ записи к объекту, уровень безопасности этого объекта доминирует над уровнем безопасности этого субъекта: $\forall s\in S, \forall o\in O, write\in M[s,o]\to F(o)\ge F(s)$.

3. Состояние безопасно тогда и только тогда, когда оно безопасно и по чтению, и по записи.

В соответствии с предложенным определением безопасного состояния критерий безопасности системы выглядит следующим образом:

Система $\Sigma(v_0,R,T)$ *безопасна тогда и только тогда, когда ее начальное состояние* v_0 *безопасно и все состояния, достижимые из* v_0 *путем применения конечной последовательности запросов из* R *безопасны.*

Белл и ЛаПадула доказали теорему, формально доказывающую безопасность системы при соблюдении определенных условий, получившую название основной теоремы безопасности.

Основная теорема безопасности Белла-ЛаПадулы.

Система $\Sigma(v_0,R,T)$ безопасна тогда и только тогда, когда:

а) начальное состояние v_0 безопасно и

б) для любого состояния v, достижимого из v_0 путем применения конечной последовательности запросов из R таких, что $T(v,r)= v^*$, $v=(F,M)$ и $v^* =(F^*,M^*)$ для каждого $s\in S$ и $o\in O$ выполняются следующие условия:

1) если $read \in M^*[s,o]$ и $read \notin M[s,o]$, то $F^*(s)\ge F^*(o)$;
2) если $read \in M[s,o]$ и $F^*(s)<F^*(o)$, то $read \notin M^*[s,o]$;
3) если $write \in M^*[s,o]$ и $write \notin M[s,o]$, то $F^*(o)\ge F^*(s)$;
4) если $write \in M[s,o]$ и $F^*(o)<F^*(s)$, то $write \notin M^*[s,o]$.

Доказательство:

1. Необходимость. Если система безопасна, то состояние v_0 безопасно по определению. Допустим, существует некоторое состояние V*, достижимое из v_0 путем применения конечного числа запросов из R и полученное путем перехода из безопасного состояния V: $T(v,r)= v^*$. Тогда, если при этом переходе нарушено хотя бы одно из первых двух ограничений, накладываемых теоремой на функцию T, то состояние V* не будет безопасным по чтению, а если функция T нарушает хотя бы одно из последних двух условий теоремы, то состояние V* не будет безопасным по записи. В любом случае при нарушении условий теоремы система небезопасна.

2. Достаточность. Проведем доказательство от противного. Пред положим, что система небезопасна. В этом случае, либо v_0 небезопасно, что явно противоречит условиям теоремы, либо должно существовать небезопасное состояние V*, достижимое из безопасного v_0 путем приме нения конечного числа запросов из R. В этом случае обязательно будет иметь место переход T(v,r)= v*, при котором состояние v — безопасно, а состояние V* — нет, однако четыре условия теоремы делают такой пере ход невозможным.

Таким образом, теорема утверждает, что система с безопасным начальным состоянием является безопасной тогда и только тогда, когда при любом переходе системы из одного состояния в другое не возникает никаких новых и не сохраняется никаких старых отношений доступа, которые будут небезопасны по отношению к функции уровня безопасности нового состояния. Формально эта теорема определяет все необходимые и достаточные условия, которые должны быть выполнены для того, чтобы система, начав свою работу в безопасном состоянии, никогда не достигла небезопасного состояния.

Состояния системы считаются безопасными (защищенными), если соотношения между уровнями защиты субъектов и ресурсов удовлетворяют как простому условию защиты, так и специальному условию.

Подсистема доступа обеспечивает безопасность, если она не допускает перехода из защищенного состояния в состояние, не являющееся защищенным. Тогда, чтобы подсистема доступа обеспечивала безопасность, необходимо и достаточно, чтобы измене-ние состояний приводило к защищенным состояниям, если исходное состояние было защищено.

Практика показывает, что многоуровневые модели защиты находятся гораздо ближе к потребностям реальной жизни, нежели матричные модели, и представляют собой хорошую основу для построения автоматизированных систем разграничения доступа. За счет более высокого "интеллекта", содержащегося в многоуровневых моделях, системы защиты с контролем доступа на уровне потоков данных во многих случаях могут без вмешательства человека принимать решения о допуске пользователей к охраняемым данным, что снижает опасность образования узких мест, связанных с деятельностью администратора защиты.

Однако в реализации многоуровневых систем разграничения доступа имеются серьезные теоретические и технические проблемы. Одна из них - возникновение состояний избыточной конфиденциальности, связанных с необходимостью периодической деклассификации (контролируемого снижения уровня секретности) конфиденциальных данных.

ОСНОВНЫЕ МАТЕМАТИЧЕСКИЕ МОДЕЛИ

1. Модель разграничения доступа в системе MULTICS

Система обработки MULTICS была разработана Массачусетским технологическим институтом по заказу Министерства Обороны США. Она предназначена для обработки информации общего и частного характера. В ЭВМ была использована кольцевая структура, размещения информации (рис. 2.2).

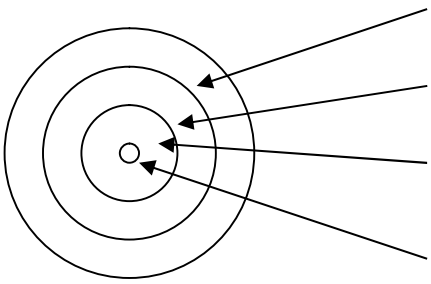


Рис.2.2. Структура размещения данных в системе MULTICS.

Программы и данные организуются в иерархические кольца, причем пользователям разрешен доступ только к кольцам на своем и более высоком уровне. Кольцевая архитектура обеспечивается аппаратными средствами изоляции. Прерывания генерируются в случае, когда пользователь нарушает допустимый уровень колец.

В данной системе функции защиты и перераспределения памяти призваны обеспечить мультипрограммирование и защищают резидентную часть программного обеспечения в оперативной памяти.

Оперативная память разделяется на защищаемую и незащищаемую области. Прикладная программа при выполнении размещается в незащищаемой области памяти и не имеет доступа в защищенную область с тем, чтобы не нарушать работу операционной системы и других программ, размещенных в этой области. Кроме того, прикладная программа не может выполнить ни одной из привилегированных команд, а это значит, что она не сможет влиять на содержимое защищенной области.

Защита областей устанавливается только с помощью программного обеспечения, находящегося в защищенной области. К программам, расположенным в защищенной области, можно обратиться только в результате прерывания. Во время прерывания программа, ранее выполнявшаяся в открытой области, может быть остановлена, и ее место может занять по усмотрению операционной системы другая прикладная программа. В этом случае операционная система изменяет границы защиты, исключив тем самым ранее выполнявшуюся программу и включив в работу очередную программу.

Функция распределения памяти позволяет выделять несколько защищенных и незащищенных областей, а при необходимости снять защиту, т.е. объявить все поле оперативной памяти незащищенным.

Нижняя граница незащищенной области указывается в регистре перераспределения базы. Содержимое этого регистра указывает также верхнюю границу нижней защищенной области. Верхняя граница незащищенной области указывается в регистре индекса защиты. Она же является и нижней границей верхней защищенной области, если она выделена. Установка границ производится специальными привилегированными командами.

Еще одной особенностью данной модели является кольцевая адресация оперативной памяти. Если адресуются ячейки, лежащие за пределами верхней границы оперативной памяти, то обращение к этим ячейкам происходит так, если бы они находились в пределах оперативной памяти. Кольцевая адресация может распространяться на определенную область оперативной памяти. Тогда попытка обращения к области, для которой кольцевая адресация отсутствует, вызывает внутренне прерывание по адресации.

2. Графовая модель защиты

Модель с графом защиты строится на понятиях графа защиты, ограниченного графа защиты и перезаписывающейся грамматики.

Граф защиты представляет собой направленный ациклический граф P(V, K), где V = (S , 0) - множество субъектов и объектов, а K - множество меток ребер, представляющих собой права доступа. Матрица смежности графа представляет собой матрицу контроля доступа.

Наряду с графом защиты, данная модель включает систему правил прибавления или удаления из графа вершин и дуг: правила "заимствования" и "передачи" прав, правила создания и удаления объекта. Эти правила описывают безопасное выполнение операций на основе перезаписывающей грамматики и соглашения о классах безопасности.

Теория графов не позволяет адекватно описать действия администратора службы безопасности. Также существенным недостатком модели является отсутствие контроля делегирования прав доступа. Модели, использующие графы защиты могут использоваться лишь в качестве вспомогательных моделей.

Контрольные вопросы

1. **Перечислите источники угроз безопасности:**

Ответ

a. антропогенные источники угроз, техногенные источники угрозы, стихийные источники угроз. (Прав.)
b. целенаправленные источники угроз, программные источники угрозы, стихийные источники угроз.
c. антропогенные источники угроз, техногенные источники угрозы, аппаратные источники угроз.

2. **Что понимают под угрозой безопасности информации**

Ответ

a. совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее.
b. целенаправленное воздействие, направленное на хищение конфиденциальной информации и/или её модификацию.

3. **Что понимают под уязвимостью информационной системы**

Ответ

a. любая характеристика или элемент информационной системы, использование которых нарушителем может привести к реализации угрозы; (Прав.)
b. не декларированные возможности информационной системы, использование которых нарушителем может привести к реализации угрозы;
c. открытые порты, использование которых нарушителем может привести к реализации угрозы.

4. **Что относиться к антропогенным источникам угроз**

Ответ

a. криминальные структуры; потенциальные преступники и хакеры; недобросовестные партнеры. (Прав.)
b. технический персонал поставщиков телекоммуникационных услуг; представители надзорных организаций и аварийных служб; представители силовых структур; (Прав.)

c. некачественные технические средства обработки информации; некачественные программные средства обработки информации; вспомогательные средства (охраны, сигнализации, телефонии);

5. Выберите варианты ответа характеризующие объективные уязвимости

Ответ

a. электромагнитные; электрические; звуковые; аппаратные закладки. (Прав.)
b. ошибки при подготовке и использовании программного обеспечения; ошибки инсталляции ПО, ошибки при управлении сложными системами.
c. нарушение режима охраны и защиты ПО нарушение режима эксплуатации технических средств; нарушение режима конфиденциальности.

6. Что относиться к техногенным источникам угроз

Ответ

a. средства связи; сети инженерных коммуникации; транспорт; некачественные программные средства обработки информации; (Прав.)
b. электромагнитные; электрические; звуковые; аппаратные закладки.
c. нарушение режима охраны и защиты ПО нарушение режима эксплуатации технических средств; нарушение режима конфиденциальности

7. Что относиться к случайным уязвимостям

Ответ

a. отказы и неисправности технических средств; старение и размагничивание носителей информации; сбои программного обеспечения; сбои электроснабжения. (Прав.)
b. ошибки при подготовке и использовании программного обеспечения; ошибки инсталляции ПО, ошибки при управлении сложными системами.
c. повреждения жизнеобеспечивающих коммуникаций; повреждения ограждающих конструкций. (Прав)

Старший преподаватель 27 кафедры
майор

С.Краснов