А. П. Дураковский, Р. С. Енгалычев

МОДЕЛИРОВАНИЕ ТИПОВЫХ УЧЕБНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ДЛЯ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ В ЧАСТИ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

В настоящий момент в открытой печати отсутствует информации о построении учебно-исследовательских лабораторных стендов, предназначенных как для организации профессиональной практической подготовки специалистов по аттестации автоматизированных систем по требованиям безопасности информации, так и для проведения исследований в области технической защиты информации в системе высшего профессионального образования.

Разработанные и распространяемые в России специальные тренажерные комплексы и специализированное программное обеспечение в основном предназначены для практического обучения (повышения квалификации) специалистов узкого профиля (специалистов по проведению отдельных видов специальных исследований, оценки защищенности и т. п.). Основным недостатком подобных комплексов является узкоспециализированный подход, направленный на получение практических навыков только по одной из типовых задач, решаемых специалистом по аттестации объектов информатизации. Также к недостаткам подобных комплексов можно отнести тот факт, что они дают специалисту только начальные знания, не позволяя провести полный комплекс исследований, направленный на получение количественных показателей защищенности, и, как следствие, произвести оценку эффективности защиты объекта.

Данная статья посвящена рассмотрению вопросов, возникающих при построении учебно-исследовательских лабораторных стендов, предназначенных для организации учебного процесса профессиональной подготовки специалистов по аттестации автоматизированных систем (АС) по требованиям безопасности информации, в части моделирования типовых защищенных АС, при описании создания специальных тренажерных комплексов и специализированного программного обеспечения по обучению способам противодействия и анализа защищенности от НСД к информации.

Рассмотрим основные задачи проектирования моделей (макетов) учебных АС:

1. Определение облика типовой учебной АС;

2. Формирование модели угроз учебной АС и определение перечня наиболее характерных угроз безопасности информации и уязвимостей, возникающих при функционировании учебной АС;

3. Определение перечня методов оценки соответствия требованиям по безопасности информации, направленных на выявление угроз безопасности информации и уязвимостей в учебной АС;

4. Определение перечня базовых подходов, методов и средств обеспечения безопасности учебной АС;

5. Определение перечня базовых подходов и методов оценки эффективности защиты информации учебной АС;

6. Определение требований по организации учебного процесса с целью комплексного обучения вопросам проведения аттестации автоматизированных систем по требованиям безопасности информации [1];

7. Определение требований к информационному обеспечению учебного процесса.

Рассмотрим наиболее существенные задачи, определяющие теоретическую и практическую ценность разрабатываемых учебно-исследовательских лабораторных стендов.

Определение облика типовой учебной автоматизированной системы

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий по проверке соответствия реализованных в АС или СВТ механизмов безопасности определенному набору требований, используемых в качестве критерия для оценки уровня защищенности АС или СВТ. В результате этих мероприятий подтверждается, что объект информатизации соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России [2–5].

При проведении аттестации АС для правильного определения ее класса необходимо ответить на четыре основных вопроса:

1) тип аттестуемой АС (однопользовательская, многопользовательская);

2) права пользователей по допуску к информации, обрабатываемой в аттестуемой АС (допущен ко всей информации, допущен только к части информации);

3) размещение информации в аттестуемой АС (на носителях одного уровня конфиденциальности, на носителях разных уровней конфиденциальности);

4) гриф секретности информации, обрабатываемой в аттестуемой АС.

Основным документом, используемым при аттестации АС, является руководящий документ ФСТЭК России (Гостехкомиссии) «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (РД для АС). Данный документ устанавливает классификацию АС исходя из ответов на вышеприведенные вопросы и содержит перечень требований по защите информации к каждому классу АС, которые для каждого из этих классов являются минимальными. Классы, в свою очередь, подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

Таблица 1. Классы и группы АС

Группа	**Описание функционирования АС и обработки в ней информации**	**Классы**
3	**Однопользовательская АС.** В АС работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности.	3Б, 3А
2	**Многопользовательская АС.** Пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности.	2Б, 2А
1	**Многопользовательская АС.** В АС одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС.	1Д, 1Г, 1В, 1Б, 1А

Исходя из классификации, приведенной в таблице 1, можно сделать вывод о том, что в ходе проведения обучения нам нужно имитировать следующие АС:

1. Однопользовательская АС (автономное СВТ, рис. 1).

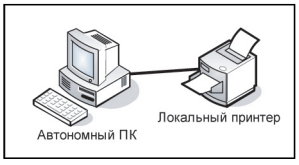

Рис. 1. Однопользовательская АС (автономное СВТ)

2. Многопользовательская АС (равноправные пользователи, объединенные в рабочую группу с возможностью использования сервера, выступающего в роли файл-сервера, почтового сервера и сервера печати, рис. 2 и рис. 3).

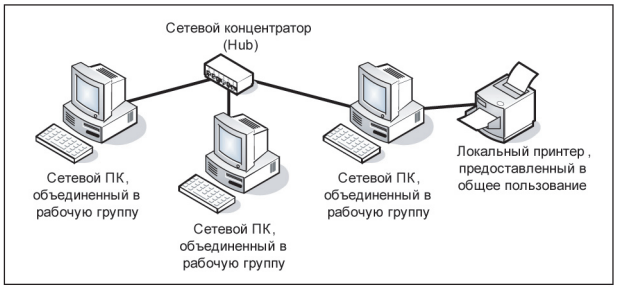

Рис. 2. Многопользовательская АС (рабочая группа без сервера)

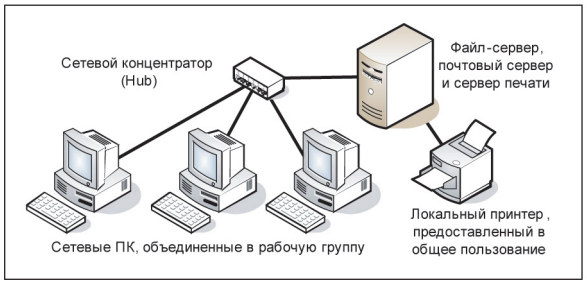

Рис. 3. Многопользовательская АС (рабочая группа с сервером)

3. Многопользовательская АС (пользователи с различными правами, объединенные в домен с возможностью использования сервера контроллера домена и сервера баз данных (БД), рис. 4).

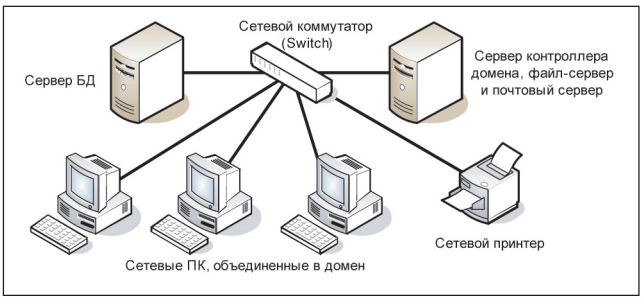

Рис. 4. Многопользовательская АС (домен с двумя серверами)

4. Многопользовательская АС (несколько доменов, объединенных в единую локально-вычислительную сеть (ЛВС), рис. 5).

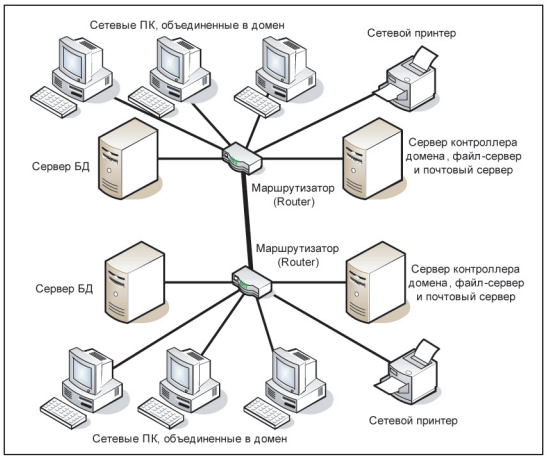

Рис. 5. Многопользовательская АС (два домена, объединенные в единую ЛВС)

Для решения поставленных задач обучения и реализации требуемых функциональных возможностей предложена схема ЛВС, содержащая (Рис. 6):

- сервер контроллера домена, одновременно выступающий в качестве файл-сервера, почтового сервера и сервера печати;
- сервер БД;
- управляемый коммутирующий маршрутизатор (switching router) с возможностью коммутации 3-го уровня (Layer 3 Switching);
- локальный лазерный принтер;
- сетевой лазерный принтер;
- несколько ПК с сетевыми картами для подключения к ЛВС.

Для сокращения затрат без ущерба для учебного процесса в качестве серверов выбраны стандартные ПК с соответствующими объемами оперативной памяти и жестких дисков, сетевыми картами, обладающими скоростями передачи данных не ниже 1000 Мбит/с.

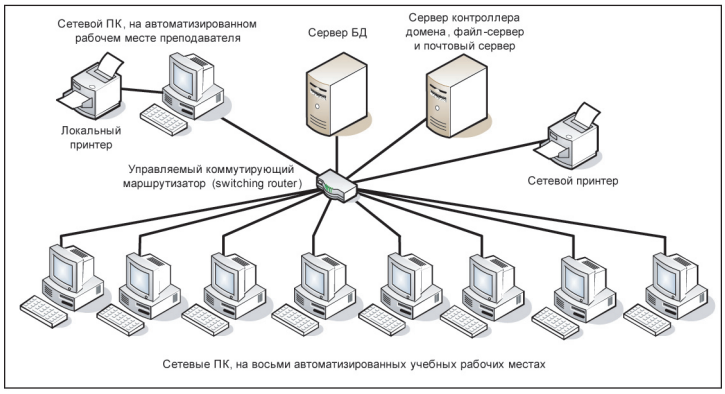

Рис. 6. Типовая АС, реализуемая в учебно-исследовательских лабораторных стендах

Каждая лаборатория имеет в своем составе 9 ПК для обеспечения работы 8 автоматизированных учебных рабочих мест и 1 автоматизированного рабочего места преподавателя, 2 сервера, которые объединяются в единую ЛВС и на которые устанавливается общесистемное и специальное программное обеспечение (ПО). В качестве операционных систем (ОС) и ПО выбраны наиболее распространенные программные продукты:

- ОС Microsoft Windows XP Russian с пакетом обновления SP3;
- пакет офисных приложений Microsoft Office 2007 Russian;
- система управления БД (СУБД) Oracle 10g.

Данный стенд позволяет моделировать все вышеприведенные модели типовых учебных АС и в ходе проведения лабораторных практикумов получать в реальных условиях следующие навыки:

1) оценка и контроль защищенности однопользовательской АС (автономного СВТ), организация ее защиты;

2) оценка и контроль защищенности многопользовательской АС (рабочая группа без/с сервером, домен, несколько доменов, объединенных в ЛВС), организация ее защиты;

3) моделирование внешних сетевых атак и защита АС с помощью межсетевого экрана;

4) контроль защищенности трафика между двумя ЛВС, организация межсетевого взаимодействия с помощью VPN-каналов.

Определение перечня наиболее характерных угроз безопасности информации и уязвимостей, возникающих при функционировании учебной АС

Под угрозами безопасности информации АС будем понимать действия или события, которые могут привести к нарушению способности АС выполнять свои функциональные задачи (ГОСТ Р

51275-2006). Угрозы безопасности есть возможности реализации воздействия на информацию, обрабатываемую АС, приводящего к дискредитации, искажению, уничтожению, копированию, блокированию доступа к информации, а также возможности воздействия на компоненты АС, приводящие к утрате, уничтожению или сбою функционирования носителя информации, средства взаимодействия с носителем или средства его управления.

Угрозы безопасности АС могут привести к нарушению:

- конфиденциальности обрабатываемой информации (информация становится известной тому, кто не располагает полномочиями доступа к ней, применение сетевых снифферов);
- целостности (злонамеренное изменение обрабатываемой информации);
- доступности (отказ в обслуживании, т. е. блокирование доступа к некоторым ресурсам АС: DoS, DDoS-атака, SYN-флуд, UDP-флуд, ICMP-флуд).

Угрозы безопасности АС могут быть реализованы как за счет технических каналов утечки обрабатываемой информации, так и за счет несанкционированного доступа к ней. Они подразделяются на преднамеренные (умышленные) и непреднамеренные (случайные). Преднамеренные угрозы информационной безопасности, в отличие от непреднамеренных, преследуют цель нанесения ущерба информационным, программным, аппаратным и другим ресурсам АС и, в свою очередь, подразделяются на пассивные и активные. Пассивные угрозы информационной безопасности имеют целью несанкционированный доступ к информации без изменения состояния АС. Пассивной угрозой является, например, перехват информации по техническим каналам утечки для последующего ее анализа. Активные угрозы имеют целью намеренное несанкционированное изменение состояния АС, например хищение или модификацию защищаемой информации (IP-спуфинг, ARP-спуфинг, атаки «Человек посередине»). В качестве источника активных угроз могут выступать также специальные средства (так называемые закладки — программные, аппаратные или программно-аппаратные), компьютерные вирусы, которые могут быть как встроены в программно-аппаратные средства АС на этапе их изготовления, так и внедрены в них преднамеренно в процессе эксплуатации, при проведении пуско-наладочных и ремонтно-профилактических работ.

Определение типовых угроз информационной безопасности, связанных с несанкционированным доступом к информации. Описание перечня учебных угроз НСД и требований к их реализации в лабораторных практикумах

К типовым угрозам информационной безопасности, связанным с несанкционированным доступом к информации, следует отнести:

1. Хищение обрабатываемой информации — несанкционированное получение (кража, копирование) нарушителем информации в процессе ее обработки, хранения или передачи.

Организационно-технические способы реализации угрозы хищения:

- кража носителей (средств документирования) информации;
- несанкционированное копирование носителей документированной информации;
- сбор и анализ информации из других источников («отходы»).

Программные способы реализации угрозы хищения базируются на специальных программных средствах, которые могут реализовывать следующие функции:

- собирать (копировать) информацию (программы) во время штатных режимов ее обработки или передачи (их функционирования);
- считывать (копировать) информацию (программы) с ее носителей;
- собирать остаточную информацию («мусор») из ОЗУ, буферов устройств или с ее носителей;
- выполнять нештатные функции по обработке информации, в частности ее размножение и переадресацию при передаче по каналам связи;
- внедрять специальные программные закладки и компьютерные вирусы.

К аппаратным средствам хищения информации относятся:

- элементы двойного назначения, которые помимо своих прямых функций дополнительно производят копирование и накопление;
- перехват информации из каналов ее передачи как внутри устройств, так и из каналов связи между устройствами;

2. Уничтожение обрабатываемой информации — несанкционированное удаление нарушителем информации в процессе ее обработки, хранения или передачи.

Программные способы уничтожения:

- стирание (перезапись) информации;
- искажение служебных данных, определяющих структуру представления (или хранения) основной (уничтожаемой) информации;
- внедрение специальных программных закладок и компьютерных вирусов.

Аппаратные способы уничтожения:

- нарушение правильности работы аппаратных средств, в результате которых происходят действия, аналогичные программным способам;
- действие специальных аппаратных закладок;
- нарушение физической целостности и аппаратной поддержки средств хранения информации (программ).

3. Блокирование обрабатываемой информации — несанкционированное изменение штатных режимов обработки и передачи информации, приводящее к невозможности выполнения в АС процедур информационного обслуживания.

Может относиться как к нарушениям, связанным с работой аппаратного оборудования, так и к отказам в программах, обеспечивающих обработку и передачу информации. Блокирование функций, обеспечивающих защиту от несанкционированного доступа, может привести и к компрометации конфиденциальных сведений.

Аппаратные способы реализации блокирования:

- нарушение (полный или частичный вывод из строя) работы аппаратного оборудования (некондиционные элементы, истечение срока эксплуатации, создание ситуаций нарушения допустимых параметров рабочего диапазона и т. д.);
- физическое разрушение или использование ненадежных каналов передачи информации;
- конструкторские просчеты при проектировании;
- неправильная сборка и настройка аппаратуры;
- ошибки в документации;
- несоблюдение эксплуатационных требований, вызывающих прекращение функционирования элементов оборудования;
- специальные аппаратные закладки, направленные на разрушение и блокирование работы элементов или узлов.

Программные способы реализации блокирования:

- ошибки (в том числе непреднамеренные) конструирования в исполнительных программах, которые приводят к некорректному выполнению функций;
- внедрение специальных программных закладок и компьютерных вирусов;
- ошибки в процессах обработки с помощью задания нестандартных режимов обработки, блокирующих работу компонентов программных систем;
- непреднамеренные ошибки пользователей и обслуживающего персонала, нарушающие правила пользования и установленные требования по эксплуатации.

4. Модификация обрабатываемой информации — несанкционированное внесение изменений в конфиденциальную информацию в процессе ее обработки, хранения или передачи, а также навязывание ложной информации.

В отличие от уничтожения или хищения в данном случае нарушитель свои действия будет осуществлять так, чтобы явно не нарушить функционирование системы или не оставить следов своей деятельности. Что касается модификации информации, то одним из возможных ее результатов может быть навязывание системе (пользователю) «ложных» сведений, которые по своей структуре и содержанию являются «легальными».

Аппаратные способы реализации модификации:

- целенаправленная замена элементов, в том числе использование элементов двойного назначения (аппаратных закладок), в техническом оборудовании;
- внесение изменений в конструкцию технических средств;
- изложение в документации неверных или неполных сведений о функционировании технического оборудования.

Программные способы реализации угрозы:

- внедрение специальных программных закладок и вирусов;
- недокументированные функции программных средств;
- непреднамеренные ошибки и преднамеренные действия пользователей и обслуживающего персонала.

5. Нарушение функционирования (элементов или узлов технических или программных средств, подсистемы в целом) — частичная или полная утрата способности элементов или узлов технических или программных средств, системы в целом к выполнению ими штатного или санкционированного режима функционирования.

Данный вид угрозы, как правило, является следствием реализации вышеперечисленных угроз в различных их сочетаниях.

Аппаратные способы реализации угрозы нарушения функционирования (разрушения) выполняются в основном с помощью различных видов физических воздействий, включая дистанционные, на оборудование посредством специализированных технических средств. Кроме того, угроза разрушения может реализоваться в результате:

- действия специальной аппаратной закладки;
- ошибочных действий обслуживающего персонала;
- нарушения правил эксплуатации, в том числе превышения предусмотренного срока эксплуатации технического оборудования;
- непредвиденной поломки оборудования из-за некачественного исполнения;
- стихийных бедствий.

В качестве учебных угроз должны быть реализованы хищение, уничтожение, блокирование и модификация обрабатываемой информации. Реализация нарушения функционирования АС как учебной угрозы представляется нецелесообразной. Учебные угрозы должны реализовываться обучающим персоналом в соответствии с методическими указаниями по их реализации, в том числе с использованием специальных аппаратно-программных средств. При этом реализация учебных угроз не должна повлечь за собой выход из строя аппаратного обеспечения учебного макета.

Определение перечня методов оценки соответствия требованиям по защите информации от НСД, направленное на выявление угроз безопасности информации и уязвимостей в учебной АС

При аттестационных испытаниях АС проводится оценка их соответствия требованиям по защите информации от НСД к информации, в том числе от компьютерных вирусов, а также иных разрушающих программных воздействий, нарушающих целостность информации или работоспособность технических средств АС.

В процессе исследований учебной АС выполняются:

- анализ и оценка технологического процесса обработки защищаемой информации;
- испытания подсистемы управления доступом;
- испытания подсистемы регистрации и учета;
- испытания подсистемы обеспечения целостности.

Анализ и оценка технологического процесса выполняются на основе следующих исходных данных:

- перечень объектов и субъектов доступа;
- перечень штатных средств доступа к информации в АС;
- перечень средств защиты информации;
- описание реализованных правил разграничения доступа;
- описание информационных потоков.

Проверяется соответствие описания технологического процесса обработки и хранения защищаемой информации реальному процессу, оценивается возможность переноса информации большего уровня конфиденциальности на информационный носитель меньшего уровня, проводится анализ разрешенных и запрещенных связей между субъектами и объектами доступа с привязкой к конкретным основным техническим средствам и системам (ОТСС) и штатному персоналу, оценка их соответствия разрешительной системе доступа персонала к защищаемым ресурсам на всех этапах обработки информации.

Проводятся испытания подсистемы управления доступом, а именно проверки:

- механизма идентификации;
- механизма аутентификации;
- реализации механизма контроля доступа.

Испытания подсистемы разграничения доступа предваряются анализом программного и аппаратного обеспечения, поиском и выявлением уязвимостей АС с помощью специализированных средств (Ревизор 1 XP, Ревизор 2 XP).

Проверка правильности идентификации субъектов доступа при входе в систему проверяется путем обращения субъектов АС к объектам доступа при помощи штатных средств. Для проверки подтверждения подлинности субъекта доступа (аутентификации) производится ввод его личного пароля. Для проверки надежности механизма аутентификации производится оценка работоспособности механизмов, затрудняющих подбор или несанкционированное получение (хищение) пароля посторонними. При испытаниях подсистемы регистрации и учета проверяется регистрация и учет событий АС, в том числе и сигнализация о попытках НСД, регистрация выдачи информации на твердую копию, а также работа механизма очистки освобождаемых областей памяти.

При испытаниях подсистемы обеспечения целостности проверяется отсутствие в АС средств отладки и разработки программ, целостность критичных файлов АС и доверенная загрузка ОС, а также реакция системы на нарушение целостности. Кроме того, выполняется проверка АС на устойчивость к заражению компьютерными вирусами.

Таким образом, в результате обучающимися будут получены не только теоретические, но и практические навыки организации комплексной защиты и проведения аттестации АС по требованиям безопасности информации.

СПИСОК ЛИТЕРАТУРЫ:

1. *Дураковский А. П., Енгалычев Р. С.* Практическая сторона вопросов подготовки специалистов по защите информации от утечки по каналу побочных электромагнитных излучений и наводок // Научная сессия МИФИ-2009. Сборник научных трудов. В 6 томах. Том V. Информационно-телекоммуникационные системы. Проблемы информационной безопасности. М.: НИЯУ МИФИ, 2009. С. 161–164.
2. Руководящий документ. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации». Гостехкомиссия России, 1992.
3. Положение по аттестации объектов информатизации по требованиям безопасности информации. Гостехкомиссия России, 1994.
4. Аттестационные испытания АС по требованиям безопасности информации. Типовая методика испытаний объектов информатики по требованиям безопасности информации (Аттестация АС). Гостехкомиссия России, 1995.
5. Руководящий документ. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». Гостехкомиссия России, 1997.