В. Р. Петров

НУЖНА ЛИ ЗАЩИТА ИНФОРМАЦИИ В СКУД?

Введение

Информационное общество характеризуется высоким уровнем развития информационных и телекоммуникационных технологий. В связи с этим состояние защищенности информационной среды, или информационная безопасность, приобретает все более актуальное значение для всех функциональных единиц государства.

Практически повсеместно задача защиты информации представляется как предупреждение несанкционированного доступа и получения ее в системах обработки данных.

В научном обеспечении большое развитие получила теория надежности [1], теория обеспечения качества информации [2], разработаны основы теории защиты информации [3].

Легко заметить, что проблема защиты информации перерастает в общую проблему управления информационными ресурсами [4].

Сегодня системы контроля и управления доступом (СКУД) широко применяются как дополнение к существующим системам защиты и охраны и представляют собой самое интенсивно развивающееся направление в технике обеспечения безопасности. Следует отметить, что функциональность систем контроля и управления доступом увеличивается год от года и в настоящее время СКУД являются одним из наиболее развитых сегментов рынка безопасности как в России, так и за рубежом.

Выбор варианта структуры и аппаратно-программных средств СКУД неразрывно связан с требованиями системной концепции обеспечения безопасности объекта. Наиболее рациональной является реализация интегрированной СКУД, так как в ней решается большинство задач автоматического управления контроля доступом, перемещения персонала, анализа попыток несанкционированного проникновения, создания разного уровня вложенных баз данных, обслуживающих службу безопасности, и т. д.

Таким образом, легко видеть, что проблема обеспечения информационной безопасности системы контроля и управления доступом любого объекта является неотъемлемой частной проблемой общей задачи обеспечения защиты объектов.

1. Исследование уязвимостей в обеспечении информационной безопасности системы контроля и управления доступом

Краткое резюме исследований, приведенное в этой части, определяет основные каналы утечки информации в СКУД, виды угроз, а также формирует основные модели потенциального нарушителя.

В общем виде все нарушения целостности информации могут происходить как преднамеренно, так и случайно. Известны следующие основные каналы утечки или нарушения целостности информации, нарушения работоспособности технических средств:

1) случайное прослушивание конфиденциальных и телефонных разговоров без использования специальных технических средств при проведении профилактических работ;

2) непреднамеренный просмотр информации с экранов дисплеев и других средств ее отображения;

3) целенаправленный несанкционированный доступ к информации;

4) побочные электромагнитные излучения информативного сигнала от технических средств и линий передачи информации;

5) наводящий сигнал на провода и линии, выходящие за пределы защищенной зоны;

6) акустическое излучение информативного речевого сигнала;

7) прослушивание телефонных и радиопереговоров;

8) воздействие на технические и программные средства в целях нарушения целостности информации, работоспособности технических средств, средств защиты информации, адресности и своевременности информационного обмена;

9) хищение технических средств с хранящейся в них информацией или отдельных носителей информации;

10) преднамеренный просмотр информации с экранов дисплеев и других средств отображения информации с помощью специальных оптических устройств;

11) визуальное наблюдение за объектом в зоне прямой видимости, в том числе с помощью фотографических и оптических средств разведки [5], [6].

2. Анализ угроз информационной безопасности системы контроля и управления доступом

Основными источникам угроз информационной безопасности в общем случае для всех объектов, и для объектов СКУД в том числе, являются: природные — стихийные бедствия и катастрофы, техногенные — отказы и неисправности технических средств и средств информатизации, человеческий фактор — деятельность человека.

Источники угроз информационной безопасности СКУД, как и для других объектов, могут быть внешними или внутренними.

Внешние угрозы исходят от природных явлений, катастроф, внешних нарушителей, лиц, входящих в состав пользователей и обслуживающего персонала СКУД.

Внутренние угрозы исходят от пользователей, обслуживающего персонала СКУД с различными правами доступа, а также от разработчиков системы.

Типы угроз, генерирующие отказы и неисправности технических средств и средств информатизации СКУД:

1. Отказы и неисправности технических средств идентификации личности, управления доступом, систем сбора и обработки информации от всех датчиков средств и систем информатизации, в том числе из-за нарушений в системе электропитания.

2. Отказы и неисправности средств защиты информации и технических средств контроля эффективности принятых мер по защите информации.

3. Сбои программного обеспечения, программных средств защиты информации и программных средств контроля эффективности мер по защите информации.

Деятельность человека — основной источник угроз по отношению к информации и СКУД:

1) Непреднамеренные действия человека:

- некомпетентные действия персонала, приводящие к ЧП и авариям;
- ошибки при проектировании СКУД и ее отдельных систем;
- ошибочные действия пользователей и обслуживающего персонала СКУД, в том числе администратора АС, приводящие к нарушению целостности и работоспособности СКУД, непреднамеренному заражению компьютеров;
- неосторожные действия персонала при техническом обслуживании или ремонте технических средств, приводящие к повреждению аппаратуры;
- неправильное обращение с магнитными носителями при использовании и хранении;
- халатность при исполнении служебных обязанностей.

2) Преднамеренная деятельность человека:

- деятельность спецслужб по добыванию информации, навязыванию ложной информации, нарушению работоспособности СКУД в целом и отдельных компонентов;

- противозаконная деятельность международных или отечественных формирований или лиц, направленная на проникновение на ядерно-опасные объекты для хищений, диверсий в отношении ядерных материалов;
- нарушение пользователями и обслуживающим персоналом СКУД установленных регламентов работы и требований информационной безопасности.

3) Преднамеренные действия вероятных нарушителей:
- хищение оборудования — частей системы;
- хищение магнитных носителей с целью копирования, подделки или уничтожения данных, получения доступа к данным и программам;
- разрушение оборудования, магнитных носителей или дистанционное стирание информации;
- считывание информации или копирование данных с носителей;
- внесение изменений в базу данных или файлы в пределах выделенных полномочий для подделки или уничтожения информации;
- считывание или уничтожение информации, ее изменение с присвоением полномочий подбором паролей при визуальном наблюдении;
- несанкционированное изменение собственных полномочий на доступ или полномочий других пользователей, минуя регламенты безопасности;
- сбор и анализ использованных распечаток, документации, других материалов и копирование ее;
- визуальный перехват информации с экранов дисплеев или клавиатуры;
- перехват электромагнитного излучения от технических средств СКУД для копирования информации и выявления процедур доступа;
- выявление паролей зарегистрированных пользователей при негласном активном подключении к кабелю локальной сети при имитации запроса сетевой операционной системы;
- установка скрытых передатчиков для вывода информации или паролей с целью копирования или доступа по легальным каналам связи с компьютерной системой в результате негласного посещения в нерабочее время или оставления их без присмотра в рабочее время;
- создание условий для разрушения информации, несанкционированного доступа к ней на разных этапах производства или доставки оборудования, разработки или внедрения системы путем включения в аппаратуру и ПО программных закладок, программ-вирусов, ликвидаторов с дистанционным управлением и т. п.;
- проникновение в систему через телефонную сеть при перекоммутации канала на модем злоумышленника после авторизации легального пользователя в сети с целью присвоения его прав на доступ к данным;
- визуальное наблюдение за объектом в зоне прямой видимости с помощью технических средств разведки.

Способы нарушения информационной безопасности СКУД могут быть:
- информационные;
- программно-математические;
- физические;
- радиоэлектронные;
- организационно-правовые.

Рассмотрим каждый из способов.

Информационные способы нарушения информационной безопасности: противозаконный сбор, распространение и использование информации; манипулирование ею (дезинформация, сокрытие, искажение); незаконное копирование, уничтожение, хищение информации; нарушение адресности и оперативности обмена, нарушение технологии обработки данных и обмена.

Программно-математические способы: внедрение программ-вирусов, «программных закладок» на стадиях проектирования и эксплуатации.

К физическим способам нарушения информационной безопасности относятся: уничтожение, хищение, разрушение средств обработки и защиты информации, средств связи, машинных и других оригиналов носителей информации; хищение ключей средств криптографической защиты; воздействие на обслуживающий персонал и пользователей системы для создания благоприятных условий для реализации угроз ИБ; диверсионные атаки на объекты информатизации.

Радиоэлектронные способы нарушения информационной безопасности включают: перехват информации в технических каналах и линиях связи, в сетях передачи данных; внедрение электронных устройств перехвата в технические средства и помещения; дезинформация по сетям передачи данных и линиям связи; подавление линий связи и систем управления.

Организационно-правовые способы нарушения ИБ — это невыполнение требований законодательства и задержки в разработке и принятии необходимых нормативных документов в области ИБ.

Наиболее опасными и реальными угрозами ИБ СКУД являются несанкционированный доступ и воздействие по отношению к информации, обрабатываемой средствами вычислительной техники и связи, а также средствам ее обработки, которые могут быть реализованы нарушителями, как персоналом СКУД, так и посторонними лицами.

Заключение

Исходя из изложенного можно сделать вывод о широком спектре угроз охраняемому объекту, его системе защиты и самой системе контроля и управления доступом как целостной системе защиты объекта. Обеспечение информационной безопасности систем контроля и управления доступом является одной из важнейших составных частей общей системы обеспечения безопасности объекта.

СПИСОК ЛИТЕРАТУРЫ:

1. *Дровникова И. Г., Буцынская Т. А.* Модель нарушителя в системе безопасности // Системы безопасности. 2008. № 5. С. 144-147

2. *Герасименко В. А., Малюк А. А.* Основы защиты информации. М.: МИФИ, 1997. — 537 с.

3. *Дружинин Г. В.* Надежность автоматизированных систем. М.: Энергия, 1977. — 536 с.

4. *Хорев А. А.* Угрозы безопасности информации // Специальная техника. 2010. № 1. [Электронный ресурс] (http://www.bnti.ru/showart.asp?aid=955&lvl=03.)

5. *Ворона В. А., Тихонов В. А.* Системы контроля и управления доступом. М.: Горячая линия — Телеком, 2010. — 272 с.

6. *Малюк А. А.* Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая линия — Телеком, 2004. — 280 с.