ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
Государственное образовательное учреждение высшего профессионального образования
«ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

РЕФЕРАТЫ ЛЕКЦИЙ В ОБЛАСТИ ФИЗИЧЕСКОЙ ЗАЩИТЫ, УЧЕТА И КОНТРОЛЯ ЯДЕРНЫХ МАТЕРИАЛОВ

ЧАСТЬ II

Учебное пособие

Издательство
Томского политехнического университета
2008

УДК 621.039.531: 004.056(075.8)
ББК 31.46я73
Р45

Авторы

В.И. Бойко, Б.П. Степанов, М.Е. Силаев, Н.Б. Егоров, Г.Н. Амелина

Р45 **Рефераты лекций в области физической защиты, учета и контроля ядерных материалов**. Часть II: учебное пособие / В.И. Бойко, Б.П. Степанов, М.Е. Силаев, Н.Б. Егоров, Г.Н. Амелина. – Томск: Изд-во Томского политехнического университета, 2008. – 18 с.

ISBN 5-98298-188-5

В учебном пособии изложено содержание лекционной части специальной дисциплины (рефераты лекций) «Автоматизированные системы физической защиты», которую в 8-м семестре изучают студенты Томского политехнического университета, обучающиеся по специальности «Безопасность и нераспространение ядерных материалов».

Пособие разработано в рамках реализации Инновационной образовательной программы ТПУ по направлению «Атомная энергетика, ядерный топливный цикл, безопасное обращение с радиоактивными отходами и отработанным ядерным топливом, обеспечение безопасности и противодействие терроризму» и предназначено для магистрантов, обучающихся по магистерским программам «Технология материалов современной энергетики» и «Физико-технические проблемы атомной энергетики» направления «Физика», а также может быть использована как руководство по самоподготовке при изучении ряда разделов указанной дисциплины студентами физических специальностей.

УДК 621.039.531: 004.056(075.8)
ББК 31.46я73

Рецензенты

Доктор химических наук,
профессор кафедры неорганической химии ТГПУ

Л.П. Ерёмин

Кандидат технических наук,
заведующий кафедрой электроники и автоматики
физических установок ТПУ
С.Н. Ливенцов

ISBN 5-98298-188-5

ПРЕДИСЛОВИЕ

Начиная с 2002 года, в ТПУ проводится обучение студентов по специальности «Безопасность и нераспространение ядерных материалов». В 2005 году подписано рамочное соглашение между ТПУ и Северо-западной тихоокеанской национальной лабораторией США (PNNL) о сотрудничестве в рамках инженерной образовательной программы по реализации в ТПУ процесса подготовки инженеров по Физической защите, учету и контролю ядерных материалов. В соответствии с программой в ТПУ при участии организаций, обозначенных Министерством энергетики США (DOE), проводятся мероприятия по становлению и совершенствованию процесса обучения по новой специальности.

Подготовка инженеров по Физической защите, учету и контролю ядерных материалов в России осуществляется в двух ведущих высших технических учебных заведениях – в Московском инженерно-физическом институте (техническом университете) и Томском политехническом университете. Учебные планы подготовки в них несколько отличаются. В ТПУ планом подготовки предусмотрено более глубокое изучение вопросов, связанных с техническими аспектами реализации концепции нераспространения ядерных материалов, то есть вопросов, касающихся технологий ядерного топливного цикла.

Данное учебное пособие представляет собой вторую часть сборника рефератов лекций по специальным дисциплинам, изучаемым студентами новой специальности, и содержит рефераты лекций по дисциплине «Автоматизированные системы физической защиты».

ЛЕКЦИЯ 1

Введение

Назначение АСФЗ и выполняемые функции. Принципы построения АСФЗ. Классификация подсистем СФЗ по назначению. Структурные схемы. Требования к техническим средствам и каналам передачи информации. Методы повышения надежности АСФЗ. Системы резервного электропитания.

При создании системы физической защиты объекта решаются следующие задачи, которые формулируются в виде целей.

1. Предупреждение, обнаружение и предотвращение несанкционированного проникновения нарушителя на объект с целью хищения или уничтожения материальных ценностей.

2. Защита объекта от воздействия стихийных сил, и прежде всего, пожара и воды.

Указанные цели могут быть достигнуты путем создания современной системы физической защиты. Существует несколько функций, которые должна решать СФЗ. К ним относятся:

1. *Обнаружение*. К функции обнаружения относится оповещение о тайных или открытых действиях нарушителей с помощью датчиков (извещателей) или систем контроля доступа.

2. *Задержка.* Выполнение этой функции состоит в замедлении продвижения нарушителей. Задержка может быть обеспечена заграждениями, замками и механическими (активируемыми) средствами задержки.

3. *Нейтрализация.* Функция, которая определяется как действия, предпринимаемые охраной для предотвращения действий нарушителей. Эффективность ответных действий во многом определяется надежностью систем связи и продолжительностью времени, необходимого для передачи сообщений.

Принципы построения АСФЗ:

- непрерывность защиты, характеризующая постоянную готовность СФЗ к отражению угроз безопасности объекта;
- активность, предусматривающая прогнозирование действий нарушителей, разработку и реализацию опережающих мер по защите;
- скрытность, исключающая ознакомление посторонних лиц со средствами и процедурами защиты;
- целеустремленность, предполагающая сосредоточение усилий по предотвращению угроз наиболее ценным составляющим объекта;
- комплексное использование различных способов и средств защиты;

- многозональность систем физической защиты, предусматривающая дифференцированный доступ различных категорий сотрудников и посетителей к составляющим объекта путем разделения его пространства на контролируемые зоны;
- многорубежность защиты, означающая, что для достижения своей цели нарушители должны обойти или преодолеть определенное количество последовательных защитных элементов (рубежей защиты);
- равнопрочность (сбалансированность) защиты, означающая, что независимо от того, каким способом нарушители попытаются достичь своей цели, им придется встретиться с эффективными элементами системы физической защиты.

В общей структуре технических средств СФЗ объектов в настоящее время выделяют следующие подсистемы.

1. Система охранной сигнализации (СОС), предназначенная для оповещения сотрудников службы безопасности и возможно других служб (например, органы вневедомственной охраны, пожарную охрану, милицию и т. д.) о проникновении нарушителя на охраняемую территорию объекта, защита от которых предусмотрена задачами системы.

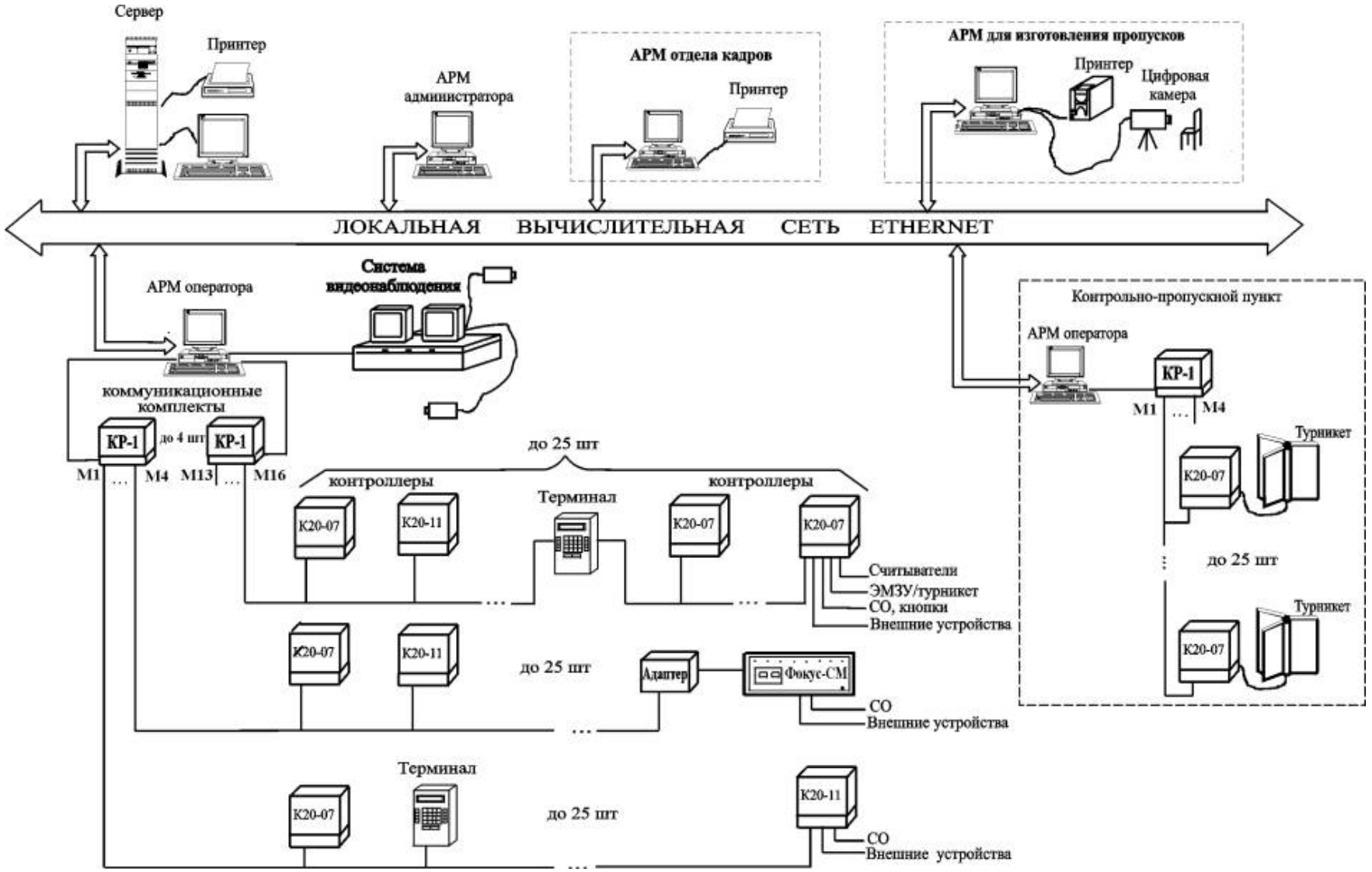
2. Система контроля и управления доступом (СКУД) представляет собой совокупность технических и программных средств, инженерно-технических сооружений и организационных мер, обеспечивающих контролируемый доступ на объект и на отдельные его составляющие, а также запрещает такой доступ всем, кто не имеет соответствующих полномочий.

3. Система телевизионного наблюдения (СТН), обеспечивающая визуальный дистанционный контроль за охраняемой территорией и действиями нарушителей. В нее также входят средства дежурного освещения, обеспечивающие необходимый уровень освещенности охраняемой территории.

4. Система связи и оповещения, предназначенная для обеспечения взаимодействия руководства предприятия, сил охраны и службы безопасности, а также для передачи данных от датчиков обнаружения СФЗ и пунктов контроля на пункт управления.

5. Подсистема сбора и обработки данных, обеспечивающая передачу сигналов тревоги, вырабатываемых датчиками обнаружения и элементами системы контроля доступа.

Современная СФЗ представляет собой гибкую, архитектурно-открытую автоматизированную интегрированную систему управления с иерархическим распределением функций по компонентам нескольких уровней (рисунок).


Сервер
Принтер
АРМ администратора
АРМ отдела кадров
Принтер
АРМ для изготовления пропусков
Принтер
Цифровая камера
ЛОКАЛЬНАЯ ВЫЧИСЛИТЕЛЬНАЯ СЕТЬ ETHERNET
АРМ оператора
Система видеонаблюдения
коммуникационные комплекты
КР-1
до 4 шт
КР-1
М1 … М4 М13 … М16
до 25 шт
контроллеры
Терминал
контроллеры
К20-07
К20-11
К20-07
К20-07
Считыватели
ЭМЗУ/турникет
СО, кнопки
Внешние устройства
К20-07
К20-11
до 25 шт
Адаптер
Фокус-СМ
СО
Внешние устройства
Терминал
К20-07
до 25 шт
К20-11
СО
Внешние устройства
Контрольно-пропускной пункт
АРМ оператора
КР-1
М1 … М4
Турникет
К20-07
до 25 шт
Турникет
К20-07

Каждое автоматизированное рабочее место (АРМ) специализировано под выполнение определенных функций за счет установки соответствующего программного обеспечения и настройки связей между составными частями системы.

АРМ операторов, работающие непрерывно в круглосуточном режиме, образуют оперативный уровень управления комплексом безопасности объекта и обеспечивают, в том числе с использованием графических планов, интерфейс пользователя для управления разнообразной периферийной аппаратурой: контроллерами, средствами обнаружения (СО), электромеханическими запирающими устройствами (ЭМЗУ), турникетами и т. п.

АРМ для изготовления пропусков на основе Prox-карт обеспечивает подготовку макетов пропусков, ввод персональных данных абонентов, в том числе ввод их фотографий с помощью цифрового фотоаппарата или сканера, печать пропусков и учетных карточек о выдаче пропуска.

АРМ администратора предназначен для конфигурирования системы, ведение базы данных абонентов с разрешительными данными, формирование и печать отчетов о событиях в системе по архиву сообщений.

АРМ отдела кадров осуществляет формирование отчетов о трудовой дисциплине (опоздание, отсутствие на рабочем месте, уход с работы ранее установленного времени) и ведет электронный табель учета использования рабочего времени.

Число АРМ любого вида в системе не ограничено. В системе обеспечивается организация АРМ с функциями, объединяющими возможности приведенных АРМ. В простейшем случае станционная часть системы может быть реализована на одной ПЭВМ.

Основой периферийной аппаратуры системы являются контроллеры, к которым подключаются считыватели пропусков, СО, кнопки экстренного вызова, отметки наряда, ЭМЗУ, турникеты, внешние устройства, управляемые релейными выходами контроллеров и т. п. Подключение контроллеров к станционной части системы осуществляется с помощью коммуникационных комплектов.

При потере связи с АРМ оператора контроллеры работают автономно, накапливая сообщения в собственном внутреннем архиве. После восстановления связи накопленная в контроллере информация передается на АРМ оператора.

Терминал представляет собой многофункциональное устройство, выполняющее в штатном режиме роль пульта управления для установки режимов охраны помещений, а при потере связи с АРМ оператора – роль ведущего устройства, управляющего подключенными к нему контроллерами. Терминал содержит базу данных абонентов, имеющих пра-

во установки режимов охраны помещений. Двухуровневая идентификация абонента осуществляется по пропуску и паролю, набираемому на клавиатуре кодонаборного устройства.

При потере связи с АРМ оператора терминал фиксирует поступление тревожного сообщения включением выходного реле (что может быть использовано для передачи на удаленную панель управления) и звукового сигнала. После регистрации пропуска с полномочиями сотрудника службы безопасности на дисплее терминала отображается системный адрес устройства, сформировавшего тревожное сообщение.

Для обеспечения совместной работы с внешними системами: видеонаблюдения, пожарной безопасности, аварийной сигнализации и др. используются стандартные интерфейсы RS–232, RS–485, Ethernet 10/100 и соответствующие драйверы.

Маловероятно, что когда-либо будет разработана такая система, в которой ни один из компонентов не откажет на протяжении всего срока ее эксплуатации. Причинами отказа компонентов системы физической защиты могут служить самые различные явления (например, факторы воздействия окружающей среды, проявление дефектов самих компонентов, целенаправленные действия нарушителей). Способы повышения надежности и живучести АСФЗ:

- блочно-модульный принцип построения системы и масштабируемость с возможностью адаптации создаваемых систем безопасности к условиям конкретного применения, а также возможность модернизации и развития в процессе эксплуатации;
- использование высоконадёжной элементной базы оборудования и полной унификации электронных модулей и блоков с контролем вскрытия корпуса;
- применение быстросъёмных конструкций, легкозаменяемых технических средств и электронных модулей;
- 100 % резервированием каналов передачи данных с использованием резервных каналов в штатном режиме для диагностического контроля, настройки технических средств и выполнения других технологических функций, а также с автоматическим переходом на резервные при неисправности основных каналов;
- возможностью передачи информации в системе по нескольким физическим линиям, по сети электропитания, по радиоканалам, по ЛВС.

ЛЕКЦИЯ 2

Системы охранной сигнализации (СОС)

Средства обнаружения в СФЗ (датчики). Классификация средств обнаружения по физическому принципу функционирования: емкостные; радиотехнические; вибрационные; акустические; оптические; контактные. Виды выходного сигнала датчиков. Системы сбора и обработки информации (контроллеры и управляющие устройства), программное обеспечение.

Система обеспечивает различные режимы управления охраной зон объекта при подключении СО, датчиков, кнопок экстренного вызова, кнопок отметки наряда и др., имеющих выход в виде нормально-замкнутой или нормально-разомкнутой контактной группы реле.

Система обеспечивает дистанционный контроль СО, имеющих соответствующие цепи управления, в автоматическом режиме до 10 раз в сутки по случайному закону и по командам с АРМ оператора.

Автоматический режим охраны внутренней зоны реализуется при оснащении всех входов в нее средствами контроля и управления доступа, при этом считыватели пропусков устанавливаются с обеих сторон точки доступа. Система автоматически распознает события: вход первого абонента в зону, выход последнего абонента из зоны. При входе первого абонента автоматически в зоне снимаются с контроля СО, которые были указаны для этой цели в процессе конфигурирования системы. При выходе последнего абонента из зоны СО ставятся на контроль. Процедуры снятия с контроля и постановки на контроль могут сопровождаться соответственно отключением и включением питания СО, если это задано при конфигурировании системы, и контроллер коммутирует питание только на СО задействованной зоны.

При централизованном управлении обеспечивается снятие с контроля и постановка на контроль индивидуально каждое СО, каждую зону. При децентрализованном управлении (с терминала) снятие с охраны и постановка на охрану осуществляется только для зоны в целом. При использовании терминалов, работающих в автономном режиме при потере связи с АРМ оператора, снятие с охраны и постановка на охрану возможны только для тех зон, в которых СО управляются контроллерами, подключенными к терминалу.

Терминал опрашивает только те контроллеры, которые физически включены за ним по магистрали.

При поступлении тревожных сообщений АРМ оператора включает звуковой сигнал, отображает графический план объекта с устройством,

сформировавшим тревогу, и выдает команды на СВН для коммутации на мониторы соответствующих ситуации телекамер, что позволяет быстро оценить ситуацию и принять адекватные меры по нейтрализации несанкционированных действий.

Функциональные характеристики системы позволяют на ее основе проектировать комплексы охранной сигнализации практически неограниченной емкости как для защиты периметров, так и внутренних зон объекта.

ЛЕКЦИЯ 3

Системы контроля и управления доступом (СКУД)

Назначение, структура и принципы функционирования подсистемы СКУД. Требования, предъявляемые к СКУД на ядерных объектах. Элементы СКУД, их взаимосвязь. Контрольно пропускные системы и исполнительные устройства. Методы и средства удостоверения личности. Считыватели как элементы системы контроля и управления доступом.

Для управления доступом в базу данных абонентов заносятся персональные сведения, включая разрешительные данные, используемые при принятии решения о доступе:

- код пропуска;
- личный код (пароль);
- номера графика работы;
- список зон, разрешенных для посещения;
- тип пропуска (постоянный, временный, разовый);
- период действия временного или разового (обезличенного) пропуска;
- номер временного графика работы;
- период времени временного графика работы.

Временные границы для разрешения доступа определяются номером графика работы. В системе предусмотрено 127 графиков работы. Каждый из них представляет собой годовой календарь, в котором на каждый день проставляется номер смены для рабочего дня или признак выходного, праздничного дня. Номер смены определяет допустимые границы времени входа и пребывания на объекте.

Для абонентов с временными или разовыми пропусками обеспечивается возможность задания права доступа только в присутствии сопровождающего.

После считывания пропуска система идентифицирует абонента, проверяет его разрешительные данные, сравнивает местонахождение считывателя и зону последней регистрации абонента (функция antipass-

back), проверяет наличие пропуска сопровождающего. При положительных результатах всех проверок доступ абоненту разрешается с уведомлением об этом на индикаторе считывателя, дисплее турникета и т. п.

При отказе в доступе формируется тревожное сообщение на АРМ оператора с указанием причины запрета доступа.

Система поддерживает реализацию алгоритма прохода с видеоверификацией, в этом случае в процедуре идентификации абонента участвует сотрудник службы безопасности (СБ) на АРМ оператора. Решение о доступе принимается по результатам сравнения фото из базы данных абонентов с изображением на мониторе СВН.

По каждому помещению системой может поддерживаться список «вскрывающих»-уполномоченных абонентов, имеющих право входа в пустое помещение, оборудованное на входе средствами контроля и управления доступом, или право управления режимами охраны помещения с терминала. При задании правила «2»…«6» лиц в пустое помещение могут войти только соответственно двое…шесть абонентов из списка «вскрывающих». После этого события в помещение могут входить все допущенные в него абоненты.

Система может поддерживать автоматический режим управления охраной требуемых помещений: при входе первого абонента в помещение снимаются с контроля СО данного помещения, при выходе последнего абонента из помещения – СО берутся на контроль.

Система обеспечивает на всей территории объекта функцию antipassback, контролирующую последовательность проходов абонентом точек доступа на основе сравнения зоны последней регистрации абонента и зоны размещения считывателя, на котором считан пропуск в текущий момент времени.

Наличие функции «antipassback» позволяет системе обнаруживать нарушения режимно-технологической дисциплины (проход через точку доступа без регистрации системой) и попытки проходов по переданному чужому пропуску.

При наличии точек доступа с односторонним контролем (считыватель на входе, кнопка на выходе), а также при нештатных и чрезвычайных ситуациях могут возникать неконтролируемые связи между зонами объекта. Система в этом случае автоматически учитывает вновь образовавшиеся зоны и сохраняет контроль за последовательностью проходов абонентом через точки доступа. Этим свойством до настоящего времени не обладала ни одна из присутствующих на российском рынке систем контроля и управления доступом. Наличие такой функции в системе является уникальным и обеспечивает существенный вклад в повышение уровня безопасности объекта.

ЛЕКЦИЯ 4

Системы телевизионного наблюдения (СТН)

Телекамеры, устройства позиционирования, системы передачи изображения, видеомониторы, записывающие устройства, системы синхронизации, системы коммутации видеоизображения, осветительная система. Структурные схемы систем видеонаблюдения. Алгоритмы обработки видеоизображения.

Система телевизионного наблюдения (СТН) как составляющая СФЗ объекта применяется для оценки ситуации на объекте. Она используется не только для наблюдения за обстановкой на объекте, но и для контроля доступа и обнаружения несанкционированного проникновения на объект, т. е. выполняет функции обнаружения и отражения.

ЛЕКЦИЯ 5

Системы связи и оповещения

Виды оперативной связи. Требования к системам связи и решаемые ими задачи. Контроль за состоянием средств обнаружения. Методы контроля состояния средств обнаружения. Необходимость защиты линии связи между средствами обнаружения и контроллерами, методы защиты линий связи, технические решения, примеры защиты линий связи.

Система связи и оповещения выполняет функцию обеспечения связи между персоналом СФЗ. В данную подсистему входят силы ответного реагирования, которые формируются из сотрудников службы безопасности объекта. В силы ответного реагирования также могут входить: милиция, вооруженные силы страны, отряды специального назначения и другие уполномоченные силы охраны объекта (например, ведомственная охрана предприятия). Силы ответного реагирования могут быть полностью или частично дислоцироваться на территории объекта или за ее пределами.

Контроль состояния линии связи на всем ее протяжении осуществляется с целью обеспечения надлежащего эксплуатационного состояния кабеля и предотвращения изменения данных в процессе их передачи. Линии связи датчиков обнаружения и аппаратуры сбора информации подразделяются на две категории – пассивные и активные.

ЛЕКЦИЯ 6

Подсистемы сбора и обработки данных

Аппаратура сбора и обработки информации от средств обнаружения (микропроцессорные контроллеры, контрольные панели) – функции, возможности, технические характеристики, методы и особенности применения. Методы интеграции устройств сбора информации и автономных подсистем СФЗ в единую систему. Правила организации пультов управления АСФЗ.

Система сбора и обработки информации осуществляет сбор данных от технических средств на объекте, представляет информацию оператору от системы телевизионного наблюдения и дает оператору возможность вводить команды управления на средства тревожного оповещения. Конечное предназначение системы сбора и обработки информации состоит в том, чтобы содействовать оперативной оценке ситуации на объекте с обнаружением причин подачи сигнала тревоги и последующим принятием соответствующих мер.

Оборудование системы сбора и обработки данных, устанавливаемое на пульте управления оператора, принимает поступающую от датчиков информацию. При проектировании пульта управления оператора необходимо ответить на следующие вопросы:

- какую информацию получает оператор:
- как представляется эта информация;
- устройства управления системой;
- расположение оборудования на АРМ оператора.

ЛЕКЦИЯ 7

Системы хранения информации

Объекты информационной безопасности, способы нарушения информационной безопасности. Защита информации в автоматизированных системах ФЗ. Методы повышения надежности хранения данных.

Проблема обеспечения безопасности информационных технологий занимает все более значительное место в реализации компьютерных систем и сетей по мере того, как возрастает их роль в информатизации общества. Это также характерно и для автоматизированных систем физической защиты, так как ценность информации, хранящейся в системе

(пароли, шифры, файлы с описанием самой системы СФЗ и т. д.), для нарушителя очень высока.

Обеспечение безопасности информационных технологий (ИТ) представляет собой комплексную проблему, которая решается в направлениях совершенствования правового регулирования применения ИТ, совершенствования методов и средств их разработки, развития системы сертификации, обеспечения соответствующих организационно-технических условий эксплуатации. Ключевым аспектом решения проблемы безопасности ИТ является выработка системы требований, критериев и показателей для оценки уровня безопасности ИТ.

Эту задачу решает новый национальный стандарт безопасности ГОСТ/ИСО МЭК 15408–2002 «Общие критерии оценки безопасности информационных технологий», действующий с 2004 г. Общие критерии (ОК) направлены на защиту информации от несанкционированного раскрытия, модификации или потери возможности ее использования. Категории защиты, относящиеся к этим трем типам нарушения безопасности, обычно называют конфиденциальностью, целостностью и доступностью соответственно. ОК могут быть также применены к тем аспектам безопасности ИТ, которые выходят за пределы этих трех понятий. ОК сосредоточены на угрозах информации, возникающих в результате действий человека как злоумышленных, так и иных, но возможно также применение ОК и для некоторых угроз, не связанных с человеческим фактором.

Профиль защиты – одно из основных понятий «Общих критериев». В привычных терминах профиль имеет много общего с техническим заданием. Все механизмы защиты, описанные в профиле, называются функциями безопасности объекта (ФБО). Проектировщик системы защиты информации выбирает необходимые ФБО для включения их в профиль из специального «каталога» функций безопасности, который входит составной частью в «Общие критерии» (2-я часть ГОСТ). Отсутствие всех остальных функций безопасности «объясняется» предположениями безопасности. Например, если компьютер с установленной программой расположен в помещении, находящемся под охраной, то часть угроз, связанных с непосредственным доступом нарушителя, можно отсекать как нереализуемые. Угрозы также выбираются из предопределенного списка и призваны обозначить, от чего именно защищает система защиты информации, соответствующая данному профилю защиты.

После разработки задания в соответствии со списком необходимых функций безопасности подбираются средства или системы защиты информации (СЗИ), реализующие данные функции. Выбранные системы

должны быть сертифицированы по ГОСТ 15408 на соответствие разработанным заданиям по безопасности.

Учитывая все вышесказанное, нетрудно заметить, что для аттестации ИС недостаточно простой установки сертифицированной ОС (например, Windows XP) на всех компьютерах организации. Необходимо разработать профиль (как минимум – задание по безопасности) на автоматизированную систему с непротиворечивой моделью угроз, политик и предположений безопасности. После этого нужно подобрать такие сертифицированные по «Общим критериям» программные продукты, функции безопасности которых позволяют защититься от описанных угроз (в числе этих продуктов уже может использоваться ОС Windows XP).

ЛЕКЦИЯ 8

Программное обеспечение интегрированных систем безопасности

Требования к программному обеспечению СФЗ и решаемые задачи. Уровни доступа и защита от несанкционированного доступа. Показатели защищенности.

Защита информации в системах ФЗ от несанкционированного доступа обеспечивается реализацией развитых механизмов контроля и управления, имеющих многоуровневую архитектуру. Наиболее часто программное обеспечение таких систем реализует трехуровневую систему защиты.

Первый уровень защиты, основанный на объединении операторов в различные по своим полномочиям группы, обеспечивается конфигурированием операционной системы автоматизированного рабочего места (АРМ). Большинству операторов предоставляется возможность работы только с ограниченным набором программных модулей, установленных в операционной системе.

Второй уровень защиты, как правило, обеспечивается системой управления базой данных (СУБД), используемой для хранения информации. Механизм защиты информации строится на возможности разграничения доступа к информации, хранящейся в таблицах базы данных. При подключении к СУБД проводится обязательная проверка подлинности клиента, после которой ему предоставляются полномочия по просмотру или редактированию данных.

Третий уровень защиты обеспечивается прикладным программным обеспечением системы. Работа любого оператора в системе ФЗ начинается с идентификации по коду пропуска и личному коду, после чего

предоставляются полномочия по управлению системой. Назначение полномочий осуществляется в программном модуле «Администратор» для каждого оператора, и эта работа может быть выполнена только администратором системы. Для каждого оператора назначается список разрешенных для работы программных модулей, а также разрешенные действия, связанные с просмотром и возможностью изменения информации и конфигурирования самой системы.

Помимо решения задач проверки подлинности, определения полномочий и контроля действий, обеспечивается ведение аудита действий операторов системы. Иными словами, информация обо всех действиях оператора сохраняется в архиве сообщений, с указанием сетевого адреса компьютера, времени, объекта действия и команд, подаваемых объекту. Кроме этого, в архив сообщений записываются все события, связанные с запуском и остановкой модулей системы и изменением прав доступа операторов. Доступ к архиву сообщений определяется полномочиями оператора.

Для защиты конфиденциальной информации ПО АСФЗ должно включать в свой состав подсистему шифрования информации. Для этой цели используются только аттестованные (сертифицированные) криптографические средства. При шифровании информации, принадлежащей различным субъектам доступа (группам субъектов), должны использоваться различные ключи. Показатели защищенности от несанкционированного доступа к информации могут быть улучшены за счет оборудования АРМ дополнительными аппаратно-программными средствами защиты, представленными на рынке.

Помимо защиты информации от несанкционированного доступа, программное обеспечение АСФЗ должно обеспечивать защиту от сбоев и искажений. Использование серверной СУБД позволяет не только значительно повысить производительность системы, обеспечить разграничение доступа к хранимой информации, но и повысить общую надежность за счет использования таких функций СУБД, как возможность восстановления информации после сбоев, «горячее» резервирование данных, возможность кластерного построения сервера базы данных, создание копии базы данных на внешних носителях.

В качестве системы управления базами данных (СУБД) могут быть использованы SQL-серверы (Interbase, MicrosoftSQL, Oracle и др.). Такое решение обеспечивает высокий уровень защищенности информации, хорошие возможности по интеграции системы в автоматизированные системы управления более высокого уровня.

СОДЕРЖАНИЕ

Учебное издание

БОЙКО Владимир Ильич
СТЕПАНОВ Борис Павлович
СИЛАЕВ Максим Евгеньевич
ЕГОРОВ Николай Борисович
АМЕЛИНА Галина Николаевна

РЕФЕРАТЫ ЛЕКЦИЙ В ОБЛАСТИ ФИЗИЧЕСКОЙ ЗАЩИТЫ, УЧЕТА И КОНТРОЛЯ ЯДЕРНЫХ МАТЕРИАЛОВ

ЧАСТЬ II

Учебное пособие

Научный редактор
доктор физико-математических наук,
профессор *И.В. Шаманин*

Редактор *Р.Д. Игнатова*
Верстка *В.П. Аршинова*
Дизайн обложки *О.Ю. Аршинова*
О.А. Дмитриев

Подписано к печати 15.12.2008. Формат 60x84/16. Бумага «Снегурочка».
Печать XEROX. Усл. печ. л. 1,05. Уч.-изд. л. 0,95.
Заказ 901. Тираж 200 экз.

Томский политехнический университет
Система менеджмента качества
Томского политехнического университета сертифицирована
NATIONAL QUALITY ASSURANCE по стандарту ISO 9001:2000

ИЗДАТЕЛЬСТВО ТПУ. 634050, г. Томск, пр. Ленина, 30.