Лабораторная работа 10. Физическая защита и защита от воздействия окружающей среды

Цель лабораторной работы: изучение важных аспектов управления ИБ организации, имеющих практическую направленность на управление физическим доступом к активам организации.

Задачи лабораторной работы:
1. Основы физической защиты информации
2 Охраняемые зоны
3. Безопасность оборудования
Контрольные вопросы

Содержание лабораторной работы:

1. Основы физической защиты информации

Физическая защита предназначена для контроля и управления физическим доступом (КУД) к активам организации. Под доступом понимается перемещение людей (субъектов доступа), транспорта и других объектов (объектов доступа) в (из) помещения, здания, зоны и территории. КУД - комплекс мероприятий, направленных на предотвращения НСД - доступа субъектов или объектов, не имеющих права доступа[1]. КУД обеспечиваются соответствующие средства контроля и управления доступом (средства КУД) - механические, электромеханические устройства и конструкции, электрические, электронные, электронные программируемые устройства, программные средства, обеспечивающие реализацию КУД. При этом средства управления - аппаратные средства (устройства) и программные средства, обеспечивающие установку режимов доступа, прием и обработку информации со считывателей, проведение идентификации и аутентификации, управление исполнительными и преграждающими устройствами, отображение и регистрацию информации. Совокупность средств КУД, обладающих технической, информационной, программной и эксплуатационной совместимостью, образуют систему контроля и управления доступом (СКУД).

При создании системы физической защиты (СФЗ) объекта решаются две важные задачи[2]:

1) *предотвращение несанкционированного проникновения нарушителя на объект с целью хищения или уничтожения активов организации;*
2) *защита объекта от воздействия стихийных сил и прежде всего, пожара и воды.*

Решение этих задач подразумевает учет большого количества различных факторов и направлено на сведение к минимуму возможностей несанкционированного проникновения на объект и к его жизненно важным центрам, вероятности осуществления актов промышленного шпионажа и последствий от воздействия стихии. Хищение и саботаж на территории объекта могут быть предотвращены двумя способами: путем удержания нарушителей от совершения нежелательных действий или путем успешного противодействия нарушителям, для чего используются соответствующие методы обнаружения (раскрытие действий, совершаемых нарушителем), задержки (замедление продвижения нарушителя) и нейтрализации (сочетание ответных действий, останавливающих нарушителей перед тем, как они выполнят свою задачу), основанные на оценке текущей ситуации на объекте.

В основу создания СФЗ положены следующие общие принципы[3]:

[1] ГОСТ Р 51241-2008 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний».
[2] Бондарев П.В., Измайлов А.В., Толстой А.И. Физическая защита ядерных объектов: учебн. пособие для вузов / Под ред. Н.С. Погожина. – М.: МИФИ, 2008.
[3] Там же

- *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.*

В общем случае структура СФЗ объектов состоит из ряда подсистем, представленных на рис. 1.

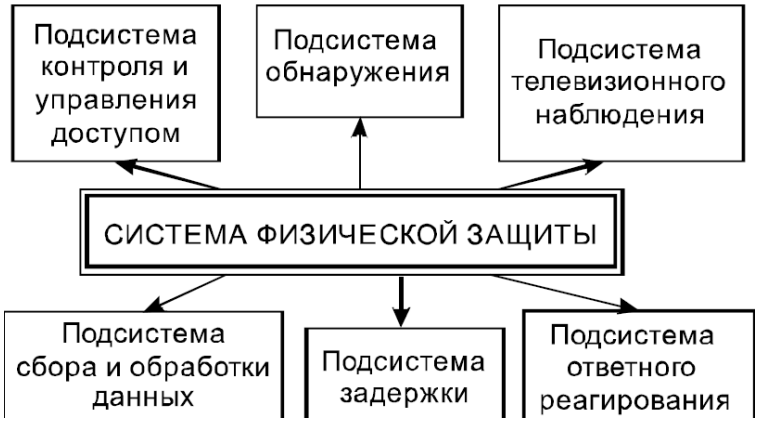

Рис. 1. Структура системы физической защиты

Таким образом, основу СФЗ составляют механические средства и инженерные сооружения, препятствующие физическому движению нарушителей к месту нахождения объектов защиты, технические средства, информирующих сотрудников службы безопасности о проникновении нарушителя в контролируемую зону и позволяющие наблюдать обстановку в них, а также средства и люди, устраняющие угрозы. Использование при создании СФЗ современных технических средств охраны и средств обработки и представления информации привело к тому, что СФЗ превратились в автоматизированные интегрированные системы безопасности, комплексно выполняющие функций обеспечения безопасности объекта.

2 Охраняемые зоны

Для физической защиты от НСД, повреждения или воздействия в отношении помещений и информации организации средства обработки критичной или важной служебной информации необходимо размещать в зонах ИБ, обозначенных определенным периметром безопасности, обладающим соответствующими защитивши барьерами и средствами контроля проникновения[4][5][6][7][8]. Уровень защищенности должен быть соразмерен с идентифицированными рисками.

Физическая защита может быть создана несколькими физическими барьерами (преградами) вокруг помещений организации и зон расположения СОИ. Барьеры

[4] ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью».

[5] ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

[6] ISO/IEC 27001:2005 «Information technology. Security techniques. Information security management systems. Requirements».

[7] ISO/IEC 27002:2005 «Information technology. Security techniques. Code of practice for information security management».

[8] Бондарев П.В., Измайлов А.В., Толстой А.И. Физическая защита ядерных объектов: учебн. пособие для вузов / Под ред. Н.С. Погожина. – М.: МИФИ, 2008.

устанавливают отдельные периметры безопасности, каждый из которых обеспечивает усиление защиты в целом. Периметр безопасности - граница, создающая барьер, например, проходная, оборудованная средствами контроля входа (въезда) по идентификационным карточкам или сотрудник на стойке регистрации. Расположение и уровень защиты (стойкости) барьера определяются по результатам оценки рисков.

В рамках физической защиты внедряются следующие мероприятия по ОИБ:

- ✓ *Периметр безопасности должен быть четко определен.*
- ✓ *Физический доступ в помещения или здания должен предоставляться только санкционированным лицам (персоналу).*
- ✓ *Периметр здания или помещений, где расположены СОИ, должен быть физически сплошным (не должно быть никаких промежутков в периметре или мест, через которые можно было бы легко проникнуть). Внешние стены помещений должны иметь достаточно прочную конструкцию, а все внешние двери – соответствующую защиту от НСД, например, оснащены устройствами контроля доступа, шлагбаумами, сигнализацией, замками и т. п.*
- ✓ *Должна быть выделенная и укомплектованная персоналом зона регистрации посетителей или должны существовать другие мероприятия по управлению физическим доступом в помещения или здания.*
- ✓ *Физические барьеры, в случае необходимости, должны быть расширены от пола до потолка, для предотвращения несанкционированных проникновений, а также исключения загрязнения окружающей среды в случае пожара или затоплений.*
- ✓ *Все противопожарные выходы в периметре безопасности должны быть оборудованы аварийной сигнализацией и плотно закрываться.*

Основные принципы, которых рекомендуется придерживаться в данной области, таковы[9]:

1) *Многозональность СФЗ, предусматривающая разбиение объекта на зоны с контролируемым уровнем защиты. Многозональность обеспечивает дифференцированный санкционированный доступ различных категорий сотрудников и посетителей к различным составляющим объекта путем разделения его пространства на контролируемые зоны. Такими зонами могут являться, например: территория, занимаемая объектом и имеющая внешнюю границу; здание на территории объекта; коридор или его часть в здании; помещение в здании.*
2) *Многорубежность защиты на пути движения нарушителя – разбиение объекта на рубежи защиты.*
3) *Равнопрочность (сбалансированность) защиты - независимо от того, каким способом нарушители попытаются достичь своей цели, им придется встретиться с эффективными элементами СФЗ.*

Пример расположения зон показан на рис. 2. Зоны могут быть независимыми (например, отдельные здания на территории объекта) или вложенными.

Совокупность многозональности и многорубежности обеспечивает эшелонированную защиту объекта - для достижения своей цели нарушители должны обойти или преодолеть определенное количество последовательных защитных элементов (рубежей защиты).

[9] Бондарев П.В., Измайлов А.В., Толстой А.И. Физическая защита ядерных объектов: учебн. пособие для вузов / Под ред. Н.С. Погожина. – М.: МИФИ, 2008.

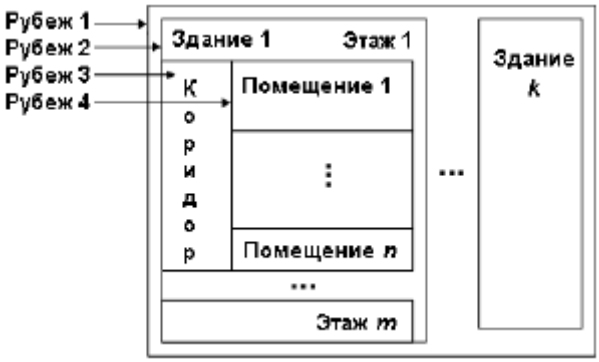

Рис. 2. Принцип многозональности и многорубежности

Охраняемые зоны ИБ защищают с помощью соответствующих мер контроля входа для обеспечения уверенности в том, что доступ позволен только авторизованному персоналу. Необходимо применять следующие меры контроля:

- *Посетители зон ИБ должны сопровождаться или иметь соответствующий допуск; дату и время входа и выхода следует регистрировать. Доступ следует предоставлять только для выполнения определенных задач. Необходимо знакомить посетителей с требованиями ИБ и действиями на случай аварийных ситуаций.*
- *Доступ к важной информации и средствам ее обработки должен контролироваться средствами КУД и предоставляться только санкционированным лицам. Следует использовать средства идентификации (запоминаемый код, биометрический признак или вещественный код). Должен надежным образом проводиться аудит журналов регистрации доступа;*
- *Весь персонал должен носить признаки видимой идентификации. Следует поощрять внимание персонала к незнакомым несопровождаемым посетителям, не имеющим идентификационных карт сотрудников.*
- *Права доступа сотрудников в зоны ИБ следует регулярно анализировать и пересматривать.*

Зона ИБ может быть защищена путем закрытия на замок самого офиса или нескольких помещений внутри физического периметра безопасности, которые могут быть заперты и иметь запираемые файл- кабинеты или сейфы. При выборе и проектировании зоны ИБ следует принимать во внимание возможные последствия от пожара, наводнения, взрыва, уличных беспорядков и других форм природного или искусственного бедствия. Также следует учитывать соответствующие правила и стандарты в отношении охраны здоровья и безопасности труда. Необходимо рассматривать и любые угрозы ИБ от соседних помещений, например, затоплений. При этом следует предусматривать следующие меры:

- ✓ *Основное оборудование должно быть расположено в местах с ограничением доступа посторонних лиц.*
- ✓ *Здания не должны выделяться на общем фоне и должны иметь минимальные признаки своего назначения - не должны иметь очевидных вывесок вне или внутри здания, по которым можно сделать вывод о выполняемых функциях обработки информации.*
- ✓ *Подразделения поддержки и оборудование, например, фотокопировальные устройства и факсы, должны быть расположены соответствующим образом в пределах зоны ИБ.*
- ✓ *Двери и окна необходимо запирать, когда в помещениях нет сотрудников, а также следует предусмотреть внешнюю защиту окон - особенно, низко расположенных.*
- ✓ *Необходимо внедрять соответствующие системы обнаружения вторжений*

(СОВ) для внешних дверей и доступных для этого окон, которые должны быть профессионально установлены и регулярно тестироваться. Свободные помещения необходимо ставить на сигнализацию. Аналогично следует оборудовать другие помещения, в которых расположены средства коммуникаций.

- ✓ *Необходимо физически изолировать СОИ, контролируемые организацией и используемые третьей стороной.*
- ✓ *Справочники и внутренние телефонные книги, идентифицирующие местоположения средств обработки важной информации, не должны быть доступны посторонним лицам.*
- ✓ *Следует обеспечивать надежное хранение опасных или горючих материалов на достаточном расстоянии от зоны ИБ. Большие запасы бумаги для печатающих устройств не следует хранить в зоне ИБ без соответствующих мер пожарной безопасности.*
- ✓ *Резервное оборудование и носители данных следует располагать на безопасном расстоянии во избежание повреждения от последствий стихийного бедствия в основном здании.*

Для усиления защиты зон ИБ могут потребоваться дополнительные меры по управлению ИБ и соответствующие руководства. Они должны включать такие мероприятия в отношении персонала или представителей третьих сторон, работающих в зоне ИБ:

- ➢ *О существовании зоны ИБ и проводимых в ней работах должны быть осведомлены только те, кому это необходимо в силу производственной необходимости.*
- ➢ *Из соображений безопасности и предотвращения возможности злонамеренных действий в зонах ИБ необходимо избегать случаев работы без надлежащего контроля со стороны уполномоченного персонала.*
- ➢ *Пустующие зоны ИБ должны быть физически закрыты и их состояние необходимо периодически проверять.*
- ➢ *Персоналу третьих сторон ограниченный санкционированный и контролируемый доступ в зоны ИБ или к средствам обработки важной информации следует предоставлять только на время такой необходимости. Между зонами с различными уровнями ИБ внутри периметра безопасности могут потребоваться дополнительные барьеры и периметры ограничения физического доступа.*
- ➢ *Использование фото, видео, аудио или другого записывающего оборудования должно быть разрешено только при получении специального разрешения.*

С целью минимизации риска НСД или повреждения бумажных документов, носителей данных и СОИ, часто внедряют политику чистого стола/экрана.

Оборудование, информацию или ПО можно выносить из помещений организации только на основании соответствующего разрешения. Там, где необходимо и уместно, оборудование регистрируют при выносе и при вносе, а также делают отметку, когда оно возвращено. С целью выявления несанкционированных перемещений активов и оборудования проводят выборочную инвентаризацию. Сотрудники должны быть осведомлены о том, что подобные проверки могут иметь место.

Во избежание НСД зоны приемки и отгрузки материальных ценностей должны находиться под контролем и, по возможности, быть изолированы от СОИ. Требования к безопасности таких зон определяются на основе оценки рисков. В этих случаях рекомендуется предусматривать следующие мероприятия:

- ✓ *доступ к зоне складирования с внешней стороны здания должен быть разрешен только определенным санкционированным лицам;*
- ✓ *зона складирования должна быть организована так, чтобы поступающие материальные ценности могли быть разгружены без предоставления персоналу поставщика доступа к другим частям здания;*

- ✓ *должна быть обеспечена безопасность внешних дверей помещения для складирования, когда внутренняя дверь открыта;*
- ✓ *поступающие материальные ценности должны быть осмотрены на предмет потенциальных опасностей прежде, чем они будут перемещены из помещения для складирования к местам использования;*
- ✓ *поступающие материальные ценности должны быть при необходимости зарегистрированы.*

3. Безопасность оборудования

Для предотвращения потерь, повреждений или компрометаций активов и ОНБ организации оборудование (включая и то, что используется вне организации) защищают от угроз ИБ, включая воздействия окружающей среды. При этом принимают во внимание особенности, связанные с расположением оборудования и возможным его перемещением. Могут потребоваться специальные мероприятия по защите от опасных воздействий среды или НСД через инфраструктуры обеспечения, в частности, системы электропитания и кабельной разводки.

При размещении оборудования реализуют следующие мероприятия по управлению ИБ:

- ➢ *Оборудование необходимо размещать так, чтобы свести до минимума излишний доступ в места его расположения.*
- ➢ *Средства обработки и хранения важной информации следует размещать так, чтобы уменьшить риск несанкционированного наблюдения за их функционированием.*
- ➢ *Отдельные элементы оборудования, требующие специальной защиты, необходимо изолировать, повышая этим общий уровень защиты;*
- ➢ *Должны быть сведены к минимуму риски потенциальных угроз ИБ, включая: воровство; пожар; взрыв; задымление; затопление (или перебои в подаче воды); пыль; вибрацию; химические эффекты; помехи в электроснабжении; электромагнитное излучение.*
- ➢ *В организации необходимо определить порядок приема пищи, напитков и курения вблизи СОИ.*
- ➢ *Важно проводить мониторинг состояния окружающей среды для выявления условий, которые могли бы неблагоприятно повлиять на функционирование СОИ.*
- ➢ *Следует использовать специальные средства защиты оборудования, расположенного в производственных цехах, например, защитные пленки для клавиатуры.*
- ➢ *Необходимо разработать меры по ликвидации последствий бедствий, случающихся в близлежащих помещениях, например, пожар в соседнем здании, затопление в подвальных помещениях или протекание воды через крышу, взрыв на улице.*

Оборудование также защищают от перебоев в подаче электроэнергии и других сбоев, связанных с электричеством. Для этого обеспечивают надлежащую подачу электропитания, соответствующую спецификациям производителя оборудования, что достигается таким образом:

- ✓ *Наличие нескольких источников электропитания.*
- ✓ *Применение устройств бесперебойного электропитания (UPS). Для безопасного выключения и/или непрерывного функционирования устройств, поддерживающих критические бизнес-процессы, рекомендуется подключать оборудование через UPS. Оборудование UPS следует регулярно проверять на наличие адекватной мощности, а также тестировать в соответствии с рекомендациями производителя. В планах ОНБ следует предусматривать действия, которые*

должны быть предприняты при отказе UPS.

- ✓ *Использование резервного генератора, если необходимо обеспечить функционирование оборудования в случае длительного отказа подачи электроэнергии от общего источника. Резервные генераторы следует регулярно проверять в соответствии с инструкциями производителя. Для обеспечения работы генератора в течение длительного срока необходимо обеспечить соответствующую поставку топлива.*

Кроме того, чтобы ускорить отключение электропитания в случае критических ситуаций, аварийные выключатели электропитания располагают около запасных выходов помещений, где расположено оборудование. Также обеспечивают работу аварийного освещения на случай отказа электропитания, потребляемого от сети. Все здания должны быть оснащены громоотводами, а все внешние линии связи оборудованы специальными грозозащитными фильтрами.

Силовые и телекоммуникационные кабельные сети, по которым передаются данные или предоставляются другие ИТ-сервисы, защищают от перехвата информации или повреждения. Для этого внедряют следующие мероприятия:

- ✓ *силовые и телекоммуникационные линии, связывающие СОИ, должны быть, по возможности, подземными или обладать адекватной альтернативной защитой;*
- ✓ *сетевой кабель должен быть защищен от несанкционированных подключений или повреждения, например, посредством использования специального кожуха и/или выбора маршрутов прокладки кабеля в обход общедоступных участков;*
- ✓ *силовые кабели должны быть отделены от коммуникационных, чтобы исключить помехи;*
- ✓ *дополнительные мероприятия по управлению ИБ для важных систем включают использование: бронированных кожухов, закрытых помещений/ящиков в промежуточных пунктах контроля и конечных точках, дублирующих маршрутов прокладки кабеля или альтернативных способов передачи, оптико-волоконных линий связи, а также проверки на подключение несанкционированных устройств к кабельной сети.*

Для обеспечения непрерывной работоспособности и целостности в организации постоянно проводится надлежащее техническое обслуживание (ТО) оборудования. В этих целях следует применять следующие меры:

- ✓ *оборудование следует обслуживать в соответствии с инструкциями и периодичностью, рекомендуемыми поставщиком;*
- ✓ *необходимо, чтобы ТО и ремонт оборудования проводились только санкционированными лицами (персоналом);*
- ✓ *следует хранить записи обо всех случаях, предполагаемых или фактических неисправностей и всех видах профилактического и восстановительного ТО;*
- ✓ *необходимо принимать соответствующие меры безопасности при отправке оборудования для ТО за пределы организации. Кроме этого должны соблюдаться все требования, устанавливаемые использующимися правилами страхования.*

Риски ИБ, например, связанные с повреждением, воровством и подслушиванием, могут в значительной степени зависеть от расположения оборудования в организации и должны учитываться при определении и выборе наиболее подходящих мероприятий по управлению ИБ. Независимо от принадлежности оборудования, его использование для обработки информации вне помещения организации санкционируется руководством. Оборудование по обработке информации включает все типы персональных компьютеров, электронных записных книжек, мобильных телефонов, а также бумагу или иные материальные ценности, которые требуются для работы на дому или транспортируются за пределы рабочих помещений. Уровень ИБ при этом должен быть эквивалентен уровню в отношении оборудования, используемого с аналогичной целью в помещениях организации, а также с учетом рисков работы на стороне. В этих условиях необходимы

следующие мероприятия по управлению ИБ:

- ✓ *оборудование и носители информации, взятые из помещений организации, не следует оставлять без присмотра в общедоступных местах. При перемещении компьютеры следует перевозить как ручную кладь и, по возможности, не афишировать ее содержимое;*
- ✓ *всегда необходимо соблюдать инструкции изготовителей по защите оборудования, например, от воздействия сильных электромагнитных полей;*
- ✓ *при работе дома следует применять подходящие мероприятия по обеспечению ИБ с учетом оценки рисков, например, использовать запираемые файл-кабинеты, соблюдать политику «чистого стола» и контролировать возможность доступа к компьютерам;*
- ✓ *должны иметь место адекватные меры по страхованию для защиты оборудования вне помещений организации.*

Более подробная информация о других аспектах защиты мобильного оборудования будем рассматривать отдельно.

Служебная информация может быть скомпрометирована вследствие небрежной утилизации (списания) или повторного использования оборудования. Носители данных, содержащие важную информацию, необходимо физически разрушать или перезаписывать защищенным образом, а не использовать стандартные функции удаления. Все компоненты оборудования, содержащего носители данных (встроенные жесткие диски), следует проверять на предмет удаления всех важных данных и лицензионного ПО. В отношении носителей данных, содержащих важную информацию, может потребоваться оценка рисков с целью определения целесообразности их разрушения, восстановления или выбраковки.

Контрольные вопросы

1. Как осуществляется физическая защита и защита от воздействия окружающей среды?
2. В чем разница понятий логического и физического доступа?
3. Как в организации создаются охраняемые зоны?
4. Что такое периметр безопасности?
5. Как защитить оборудование организации от различных видов угроз?

Задание

Отчет по лабораторной работе выполняется по стандарту, описанному в методических указаниях