ВОПРОСЫ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Марков Георгий Алексеевич, *инженер ОАО «Концерн «Системпром», г. Москва,*
E-mail: gm@cnpo.ru

Публикация продолжает серию статей по подготовке к сдаче экзамена на статус сертифицированного специалиста по информационной безопасности (Certified Information Systems Security Professional) [1–9]. Рассмотрены вопросы физической безопасности ресурсов ИТ–организаций. Рассмотрен перечень основных сегментов организации, требующих физической защиты, к каждому из которых даются основные определения, классификации и рекомендации. При этом основной целью публикации является структуризация предметной области физической безопасности для облегчения подготовки к экзамену именно ИТ–специалистам. Даны рекомендации по успешной сдаче экзамена CISSP.

Ключевые слова*: информационная безопасность, физическая безопасность, физическая защита информации, CISSP.*

ISSUES OF PHYSICAL AND ENVIRONMENTAL SECURITY

Georgii Markov*, Engineer at Concern Systemprom, Moscow,*
E-mail: gm@cnpo.ru

This publication continues our series of articles for information security specialists, preparing to take an exam for Certified Information Systems Security Professional certification [1–9]. The questions of physical and environmental security of IT organizations are considered. The list of the main segments of the organization requiring the physical protection is given. The basic definitions, classifications and recommendations are presented. Thus the main purpose of this publication is the structuring of the subject area of physical security to facilitate the preparation for the exam. The recommendations for a successful exam CISSP are given.

Keywords*: information security, physical security, physical protection, CISSP.*

Введение

Обеспечение безопасности ресурсов компьютерных систем существенно затруднено в случае физического соприкосновения злоумышленника с системой. Кроме того, уровень информационной безопасности организации может быть снижен также в результате непреднамеренных физических повреждений инфраструктуры и ресурсов системы. По этой причине вопросы физической безопасности затрагиваются в рамках курса CISSP как обязательный атрибут доверия к компьютерным системам [10, 11].

К сожалению, на практике в политиках безопасности ИТ-организации вопросы физической безопасности отражаются неполно или вообще выносятся за рамки технической защиты информации. В то же время администраторы безопасности зачастую знакомы с отдельными вопросами физической безопасности, связанных, например, с эксплуатацией системы источников бесперебойного питания и установкой кодовых замков. Однако курс CISSP предполагает более систематизированные знания, касающиеся базовых принципов физической безопасности ИТ-организации. В этом смысле физическую безопасность можно считать фундаментом в организации безопасности ИТ-организации: некоторые специалисты рекомендуют даже начинать подготовку к получению сертификата CISSP с данного раздела [1].

Угрозы физической безопасности

Традиционно угрозы делят на естественные (природные), искусственные (техногенные), а последние – на случайные и преднамеренные [2]. Однако на классификацию угроз физической безопасности повлияли различные службы, исторически сложившиеся еще до формирования понятия компьютерной безопасности. Например, в рамках физической безопасности выделяют угрозы:

- угрозы систем обеспечения ИТ-организации (электричества и связи);
- угрозы пожаробезопасности;
- угрозы, связанные с персоналом и т.д.

По территориальному признаку угрозы делят на внутренние и внешние.

Отметим базовые принципы физической безопасности.

Как и в других разделах CISSP в области физической безопасности основным приоритетом в обеспечении безопасности является человек как главный актив, а значит, цели защиты жизни и здоровья работников и клиентов должны иметь приоритет.

Другим важным принципом является приверженность многоуровневой модели защиты («эшелонированной обороны»), где при нарушениях на одном из уровней защиты ресурсы будут защищены другими.

Физическую безопасность, также как многие другие вопросы информационной безопасности, удобно рассматривать в рамках модели PDCA (plan, do, control, act), эффективность которой задается первым этапом – планированием [3].

Планирование физической безопасности

После положительного решения со стороны руководства о необходимости обеспечения физической безопасности организации формируется группа разработчиков программы физической безопасности, которая (совместно с руководством) должна определить основные цели программы, а также показатели, по которым данная программа будет оцениваться после создания на предмет того, что все поставленные цели достигаются. В формируемой этой группой программе должны учитываться следующие цели:

- предотвращение преступлений и разрушений посредством сдерживания (устрашения);
- уменьшение повреждений посредством использования задерживающих механизмов;
- выявление вторжений или повреждений;
- оценка инцидентов;
- процедуры реагирования.

Предотвращение преступлений

Одним из методических подходов, наиболее часто используемых при разработке программы физической безопасности, является «Предотвращение преступлений посредством проектирования окружения» - CPTED (Crime Prevention Through Environmental Design). Данный подход преследует цель: как правильно спроектировать физическое окружение, чтобы снизить вероятность преступлений, и предлагает три стратегии:

- естественное управление доступом;
- естественное наблюдение;
- естественное укрепление территории.

Естественное управление доступом (natural access control) - это стратегия, направленная на управление доступом людей на территорию и объекты.

Естественное наблюдение - это стратегия, направленная на обеспечение максимальной видимости территории вокруг здания. Цель данной стратегии - создание некомфортных условий для злоумышленника.

Естественное укрепление территории (natural territorial reinforcement) - это стратегия, направленная на создание физического защитного окружения.

Защитные механизмы

Как правило, все элементы защиты делят на внутренние и внешние.

Внутренние элементы физической безопасности включают в себя следующие:

- системы отопления, вентиляции и кондиционирования воздуха (HVAC, Heating, Ventilation, & Air Conditioning);
- материал, из которого изготовлены стены, фальшпол и потолки;
- системы распределения электроэнергии;
- схемы и виды коммуникаций (например: медный кабель, телефонный кабель, оптоволокно и т.п.);
- использование опасных материалов.

К внешним элементам физической безопасности относят следующие:

- расположение аэропортов, автомагистралей, железных дорог;
- электромагнитные помехи от окружающих устройств;
- климатические особенности;
- грунт;
- существующие ограждения, датчики движения, камеры, барьеры;
- транспортная активность;
- соседи.

Организация может иметь ответственного за безопасность здания - FSO (facility safety officer), который должен иметь полную информацию о здании, а также о требованиях, которым должна соответствовать компания.

Особенности физической безопасности, связанные со зданиями

При выборе места для здания нужно обратить внимание на следующие области:

- видимость (окружающая местность, население, типы соседей и пр.);

- окружающая область и внешние объекты (близость медицинских учреждений, угрозы окружающей среды и пр.);
- доступность (дороги, расположение вокзалов и аэропортов и пр.);
- природные катастрофы (вероятность стихийного бедствия).

В процессе проектирования здания следует обратить внимание на конструктивные компоненты, а именно:

- стены (горючесть материала, пожарный рейтинг и пр.);
- двери (горючесть материала, сопротивление силовым воздействиям, размещение и пр.);
- потолки (горючесть материала, нагрузочный рейтинг и пр.);
- окна (защита от разбивания, размещение и пр.);
- пол (горючесть материала, нагрузочный рейтинг и пр.);
- отопление, вентиляция и кондиционирование воздуха;
- источники электроэнергии;
- водопровод и газопровод;
- устройства обнаружения и тушения пожара.

По известным причинам особое внимание уделяется конструктивным особенностям дверей. Так, если рассматривать двери по предназначению, то можно сделать следующее разделение:

- двери хранилища;
- двери для прохода персонала;
- промышленные двери;
- двери для проезда автомобилей;
- пуленепробиваемые двери.

Важным моментом является защита петель и пластин замков. Например, на петли нужно закрепить заклепки, которые нельзя удалить.

Для блокирования проникающих несанкционированно посетителей рекомендуется использовать шлюзы и турникеты. Шлюз (mantrap) - это маленькая комната с двумя дверями. При прохождении первой двери происходит ее блокирование, а при успешной аутентификации или распознавания вторая дверь открывается.

Многие двери имеют автоматические замки, которые имеют две настройки: на защиту персонала (fail-safe) и на защиту активов (fail-secure). Настройка двери на безопасность персонала означает, что при отключении электропитания двери автоматически открывается. Настройка двери на защиту активов означает, что при отключении электропитания двери остаются закрытыми.

Следующими после дверей по важности идут окна. Существуют следующие типы окон:

- стандартное (без дополнительной защиты, дешевое, минимальный уровень защиты),
- закаленное (стекло нагревается, а затем быстро охлаждается для увеличения прочности),
- акриловое (разновидность пластика вместо стекла),
- армированное (наличие между двумя стеклами проволочной сетки, которая предотвращает разбитие или разрезание стекла),
- многослойное (между стеклами устанавливается пластик для защиты от разбивания),
- пленка, защищающая от солнечного света (защита от разбивания и безопасность за счет тонирования),
- защитная пленка (прозрачная пленка, усиливающая стекло).

Рекомендации по защите систем поддержки и снабжения

Как отмечалось, к системам поддержки обычно относят системы электроэнергии и пожаротушения.

Рассмотрим кратко вопросы электроэнергетической безопасности. Имеется три основных метода и соответственные средства защиты от проблем электроснабжения:

- источники бесперебойного питания (ИБП, UPS - Uninterruptible Power Supply);
- устройства защиты от электрических помех;
- резервные источники электроэнергии.

Среди ИБП выделяют линейные и линейно-интерактивные ИПБ.

Линейные ИПБ (online UPS system) для зарядки своих батарей используют напряжение сети переменного тока. Такой ИПБ быстро выявляет проблему электропитания, так как через него постоянно проходит электричество. В сравнении с линейно-интерактивным, линейный ИПБ восстанавливает электропитание быстрее.

Линейно-интерактивные ИПБ (standby UPS) не активны до возникновения проблем с электропитанием (такие проблемы выявляются при помощью соответствующих датчиков). Восстановление электропитания происходит медленнее, чем при использовании линейного ИПБ из-за того что при переключении к батареям происходит задержка. Линейно-интерактивные ИПБ менее функциональны, но имеют более низкую цену.

Понятно, что резервные источники питания нужны для ситуаций, когда проблемы с электропитанием продолжаются дольше, чем может работать ИПБ.

Что касается прерываний и помех электроэнергии, то здесь различают четыре вида перепадов на-

пряжения электрического тока:

- превышение напряжения, к которому относят:
- пик (spike) - кратковременный скачок напряжения;
- перенапряжение (surge) - длительное повышение напряжения;
- потеря напряжения, в том числе:
- перебой (fault) – кратковременное отсутствие напряжения;
- отключение (blackout) - длительное отсутствие напряжения;
- снижение напряжения:
- проседание/спад (sag/dip) - кратковременное снижение напряжения от одного цикла до нескольких секунд;
- провал (brownout) - длительное снижение напряжения ниже нормального уровня;
- пусковой ток (in-rush current) - первоначальный скачок тока, необходимый для запуска механизма.

Рассмотрим кратко вопросы пожарной безопасности.

Выделяют четыре класса пожара:

- класс A, касающийся горения обычных материалов;
- класс B, связанный с горением горючей жидкости, например, бензина;
- класс C, связанный с наличием электрического оборудования и проводов;
- класс D, связанный с особыми горючими материалами, например выделяющими кислород при горении.

Средства тушения указанных классов представлены в табл.1.

В табл. 2 представлены способы и средства тушения различных веществ.

Кратко покажем классификацию огнетушителей. Огнетушители классифицируются по следующим особенностям:

- по величине массы и способу доставки к месту возгорания:
- переносные (до 20 кг.);
- передвижные (от 20 до 400 кг.);
- по типу применяемого вещества:
- водные;
- пенные;
- порошковые;
- газовые;
- комбинированные;
- по принципу вытеснения огнетушащего вещества:
- закачные;
- с баллоном сжатого или сжиженного газа;
- с газогенерирующим элементом;
- с термическим элементом;
- с эжектором;
- по значению давления:
- низкого давления;
- высокого давления;
- по способу востановления технического ресурса:
- перезаряжаемые;
- неперезаряжаемые;
- по назначению (для тушения различных классов пожара).

Важным моментом обеспечения пожарной безопасности является выбор типа водяного сприн-

Таблица 1. *Классы пожаров и средств их тушения*

Класс пожара	Тип	Горящие материалы	Тушение
A	Обычные горючие вещества	Дерево, бумага и пр.	Вода, пена
B	Жидкости	Нефтепродукты	Газ, пена, порошок, CO2
C	Электрический	Электрическое оборудование и провода	Газ, порошок, CO2
D	Горючие материалы	Натрий, магний, калий	Порошок

Таблица 2. *Средства тушения пожара различными веществами*

Компонент пожара	Средство тушения	Как происходит тушение
Топливо	Углекислый натрий	Удаляет топливо
Кислород	CO2	Удаляет кислород
Температура	Вода	Снижает температуру
Химическая реакция горения	Хладон или его заменители	Препятствует химической реакциям между элементами

клера (sprinkler - разбрызгиватель), к которым относят следующие:

- системы с «мокрыми» трубами (wet pipe), которые держат воду в трубах (минусом системы является возможность заморозки воды в трубах при низких температурах);

- системы с «сухими» трубами (dry pipe), которые не держат воду в трубах;

- упреждающие (preaction) системы, в которых вода держится до момента расплавления тепловой пробки в головке сплинклера (т.е. предоставляется время персоналу на тушение не сильного пожара огнетушителями);

- поточные (deluge) системы, которые имеют широкие спринклерные головки, за счет чего выпускают больший объем воды в единицу времени.

Рекомендации по физической защите доступа на объекты

Здесь обычно разделяют на средства закрытия доступа к ресурсам (например, замки) и средства защиты периметра (например, ограждения).

Замок является задерживающим недорогим устройством для нарушителей. Существует два основных типа механических замков:

- с нарезкой;

- цилиндровые.

Замок с нарезкой (warded lock) – это обычный висячий замок, оснащенный пружинной задвижкой с вырезанным в ней пазом. Цилиндровый замок (tumbler lock) имеет больше частей и элементов, чем замок с нарезкой. Цилиндровый замок делится на три вида:

- пиновые (штифтовые),

- пластинчатые;

- сувальдные (lever tumbler lock).

Кроме механических выделяют кодовые и шифр-замки. Кодовые замки (combination lock) требуют ввода правильного сочетания цифр для их открытия. Шифр-замки (cipher lock) - используют клавиатуру для контроля доступа в помещение или здание.

Большинство шифр-замков обладают следующими возможностями:

- дверной таймер (door delay) - при открытии двери дольше определенного времени, будет подан сигнал для оповещения персонала безопасности о подозрительной деятельности;

- замещение ключа (key override) - возможность запрограммирования специальной комбинации для использования в чрезвычайных ситуациях с целью обхода обычных процедур или контроля;

- мастер-ключ (master keying) - ключ для изменения кодов доступа и других функций шифр-замка;

- открытие под принуждением (hostage alarm) - возможность ввода специальной комбинации, указывающей персоналу по безопасности об открытии замка под принуждением.

Кроме замков в области физической безопасности широко используются блокирующие устройства. Приведем примеры основных типов блокирующих устройств:

- защита кнопок включения (switch control) - закрытие кнопок, отвечающих за включение и отключение устройства;

- защитные слоты (slot lock) - защищает устройство от хищения путем закрепление стального кабеля;

- защита портов (port control) - блокировка доступа к дисковым устройствам и неиспользуемым портам;

- защита включения периферийных устройств (peripheral switch control) - защита клавиатуры, путем установки переключателя (включено/выключено) между системным блоком и клавиатурным разъемом;

- кабели-ловушки (cable trap) – защита от извлечения устройств ввода/вывода, устанавливая их кабели через блокирующее устройство.

Следует отметить, что в области физической безопасности для хранения носителей информации и отдельных серверов могут использоваться специальные сейфы.

В общем плане сейфы делятся на два типа: огнестойкие и взломостойкие.

Цель огнестойких сейфов - это сохранность документов в течении времени при больших температурах. Взломостойкие направлены на сопротивляемость полному или частичному вскрытию при помощи различных инструментов.

Отметим, что существуют огнезломостойкие сейфы, которые совмещают устойчивость как к пожарам, так и к взломам. Такие сейфы достаточно дороги, так как обеспечить двойную защиту в одном сейфе крайне трудно. Кроме того, такие сейфы имеют меньший объём при одинаковых размерах в сравнении с другими сейфами, так как имеют утолщенные стенки.

В рамках защиты периметра обычно рассматривают ограждение, освещение и видеонаблюдение.

Различная высота ограждений соответствует соответствующему уровню защиты:

- от 3 до 4 футов (0,9 – 1,2 метра) - сдерживает только случайных нарушителей.

- от 6 до 7 футов (1,8 – 2,2 метра) - через такое

ограждение уже тяжело перелезать, что может остановить злоумышленника.

- от 8 футов (2,5 метра) - сдерживает даже решительного злоумышленника.

При установке освещения нужно помнить, что оно должно быть направлено наружу на области, из которых наиболее вероятно будет действовать нарушитель.

В заключение подраздела следует упомянуть системы видеонаблюдения (CCTV - closed-circuit TV).

Основная цель системы видеонаблюдения состоит в выявлении, оценке и/или идентификации нарушителей. При выборе устройства видеонаблюдения следует учесть следующие моменты:

- тип окружения, в котором будут работать камеры видеонаблюдения: внутренние помещения или внешние области;

- область обзора: широкая или узкая;

- величина освещенности окружения: светлые или темные области;

- интеграция с другими механизмами контроля безопасности: охрана, IDS, системы сигнализации.

Нормативные документы

В рамках подготовки к сдаче экзамена CISSP следует знать основные стандарты в области информационной безопасности. Относительно физической безопасности ИТ-организации наиболее более релевантным следует назвать приложение A9 к ISO 27002, включающее практические рекомендации в области менеджмента информационной безопасности, касающиеся физической безопасности (Physical and Environmental Security). Рекомендации включают две части: безопасные зоны (Secure Areas) и защиту оборудования (Equipment).

Кроме того, вопросы физической безопасности отражены в COBIT5 (процессы BAI 09, DSS 05), NIST SP 800-53 (контроли: Physical and Environmental Protection), а также можно рекомендовать стандарты и учебные материалы охранной ассоциации ASIS International.

В нашей стране имеется национальный стандарт ГОСТ Р 52860-2007 «Технические средства физической защиты. Общие технические требования», ориентированный, правда, на средства физической безопасности, применяемые в системах защиты ядерных объектов.

Заключение

В данной статье мы рассмотрели наиболее востребованные вопросы и классификации в области физической безопасности, которые надо знать соискателю сертификата CISSP. За рамками статьи остались средства контроля (идентификации) доступа, частично рассмотренные в разделе по безопасности доступа [8], вопросы физической устойчивости организации, упоминаемые в домене по непрерывности бизнеса [9], технические средства защиты информации от утечек по техническим каналам (особенно вариации по теме TEMPEST - Transient Electromagnetic Pulse Emanation Standard), а также физические типы атаки, как-то: взлом замков, подключение к каналам связи, отвлечение охранников и собак и др.

Литература:

1. Дорофеев А.В. Статус CISSP: как получить и не потерять? // Вопросы кибербезопасности. 2013. № 1(1). С.65-68.
2. Дорофеев А.В., Марков А.С. Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. № 1 (2). С. 67-73.
3. Дорофеев А.В. Менеджмент информационной безопасности: управление рисками // Вопросы кибербезопасности. 2014. № 2(3). С.66-73.
4. Дорофеев А.В. Менеджмент информационной безопасности: переход на ISO 27001:2013 // Вопросы кибербезопасности. 2014. № 3(4). С.69-73.
5. Дорофеев А.В. Подготовка к CISSP: телекоммуникации и сетевая безопасность // Вопросы кибербезопасности. 2014. № 4(7). С. 69-74.
6. Барабанов А.В. Подготовка к сдаче CISSP: модели информационной безопасности // Вопросы кибербезопасности. 2014. № 5(8). С. 59-67.
7. Марков А.С., Цирлов В.Л. Основы криптографии: подготовка к CISSP // Вопросы кибербезопасности. 2015. № 1 (9). С. 65-73.
8. Марков А.С., Цирлов В.Л. Безопасность доступа: подготовка к CISSP // Вопросы кибербезопасности. 2015. № 2 (10). С. 60-68.
9. Дорофеев А.В., Марков А.С. Планирование обеспечения непрерывности бизнеса и восстановления // Вопросы кибербезопасности. 2015. № 3 (11). С. 68-73.
10. Good Practice Guidelines 2013 Global Edition. A Guide to Global Good Practice in Business Continuity / by ed. L.Bird. BCI. 2013. 116 p.
11. Tipson H.F. Official ISC2 Guide to the CISSP CBK, 4th ed. ICS2. 2009. 968 p.

References:

1. Dorofeev A.V. Status CISSP: kak poluchit' i ne poteryat', Voprosy kiberbezopasnosti, 2013, No 1(1), pp.65-68.
2. Dorofeev A.V., Markov A.S. Menedzhment informatsionnoy bezopasnosti: osnovnye kontseptsii, Voprosy kiberbezopasnosti, 2014, No 1 (2), pp.67-73.
3. Dorofeev A.V. Menedzhment informatsionnoy bezopasnosti: upravlenie riskami, Voprosy kiberbezopasnosti, 2014, No 2(3), pp.66-73.
4. Dorofeev A.V. Menedzhment informatsionnoy bezopasnosti: perekhod na ISO 27001:2013, Voprosy kiberbezopasnosti, 2014, No 3(4), pp.69-73.
5. Dorofeev A.V. Podgotovka k CISSP: telekommunikatsii i setevaya bezopasnost', Voprosy kiberbezopasnosti, 2014, No 4(7), pp.69-74.
6. Barabanov A.V. Podgotovka k sdache CISSP: modeli informatsionnoy bezopasnosti, Voprosy kiberbezopasnosti, 2014, No 5(8), pp.59-67.
7. Markov A.S., Tsirlov V.L. Osnovy kriptografii: podgotovka k CISSP, Voprosy kiberbezopasnosti, 2015, No 1 (9), pp.65-73.
8. Markov A.S., Tsirlov V.L. Bezopasnost' dostupa: podgotovka k CISSP, Voprosy kiberbezopasnosti, 2015, No 2 (10), pp.60-68.
9. Dorofeev A.V., Markov A.S. Planirovanie obespecheniya nepreryvnosti biznesa i vosstanovleniya, Voprosy kiberbezopasnosti, 2015, No 3 (11), pp.68-73.
10. Good Practice Guidelines 2013 Global Edition. A Guide to Global Good Practice in Business Continuity / by ed. L.Bird. BCI, 2013. 116 p.
11. Tipson H.F. Official ISC2 Guide to the CISSP CBK, 4th ed. ICS2. 2009. 968 p.