МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
Дальневосточный федеральный университет

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Кафедра информационной безопасности

О Т Ч Е Т

о прохождении учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики

Выполнил студент
гр. С8118-10.05.01-1СПЕЦ
_____ Цегельников И.А.
(подпись)

Отчет защищен с оценкой

_____
_____ С.С. Зотов
(подпись) (И.О. Фамилия)
« 31 » июля 2021 г.

Руководитель практики
Старший преподаватель кафедры
информационной безопасности ШЕН
_____ С.С. Зотов
(подпись) (И.О. Фамилия)

Регистрационный № _____
« 31 » июля 2021 г.

_____ Е.В. Третьяк
(подпись) (И.О. Фамилия)

Практика пройдена в срок
с « 19 » июля 2021 г.
по « 31 » июля 2021 г.
на предприятии
Кафедра информационной безопасности ШЕН ДВФУ

г. Владивосток
2021

Содержание

Задание на практику

- Провести исследования в области организации физической безопасности информационных ресурсов.

- Написание отчета по практике о проделанной работе.

Введение

Учебная (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практика проходила на кафедре информационной безопасности ШЕН ДВФУ в период с 19 июля 2021 года по 31 июля 2021 года.

Целью прохождения практики является приобретение практических и теоретических навыков по специальности, а также навыков оформления проведенного исследования в отчетной форме.

Задачи практики:

1. Ознакомиться с нормативной базой по организации физической безопасности информационных ресурсов.
2. Теоретически ознакомиться с методами организации физической безопасности информационных ресурсов и методами их работ.
3. На основе полученных знаний написать отчет по практике о проделанной работе.

Организация физической безопасности информационных ресурсов.

Organization of physical security of information resources.

Аннотация:

Защита данных, которая требует разработку инновационных и модернизации существующих методов противодействия противозаконным действиям, имеет огромную актуальность на сегодняшний день. Главной целью данной статьи является исследование актуальных вопросов, касающихся физической защиты информации. Второстепенными задачами данной работы являются: выделение проблем физической защиты информации, а также предложения для решения проблем.

Предисловие:

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. Физическая безопасность информационных ресурсов направлена, в первую очередь, на предотвращение неавторизованного доступа, повреждения и воздействия в отношении помещений и информации организации, а также на обеспечение безопасности средств обработки критичной служебной информации, посредством использования различных средств контроля проникновения, а также защитных барьеров.
Для того чтобы грамотно построить физическую безопасность своих информационных ресурсов надлежащим образом необходимо понять основные угрозы безопасности, а также методы их решения.

Актуальность:

Информационные технологии являются одним из ключевых векторов развития практически всех сфер жизнедеятельности современного человека. Именно посредством эффективной работы алгоритмов защиты информационных потоков достигается рациональная и бесперебойная деятельность современных автоматизированных предприятий.

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.

Отметим базовые принципы физической безопасности.

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.

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;

- 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 offi cer), 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.

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 **огневзломостойкие** 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

В данной статье мы рассмотрели наиболее востребованные вопросы и классификации в области физической безопасности

Заключение

Для достижения данной цели, в процессе прохождения учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики познакомился с организацией физической безопасности информационных ресурсов, с методами организации физической безопасности информационных ресурсов, а также способами их работ.

Также были изучены требования к написанию отчета по практике. В результате прохождения практики был составлен отчет по практике, соответствующий предъявленным требованиям.

В ходе прохождения практики все задачи были выполнены, а цель достигнута.

Список используемых источников

1) Научная электронная библиотека Elibrary.ru https://elibrary.ru/project_risc.asp
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., Марков А.С. Планирование обеспечения непрерывности бизнеса и восстановления // Вопросы кибербезопасности. 2015. № 3 (11). С. 68-73.
6) Good Practice Guidelines 2013 Global Edition. A Guide to Global Good Practice in Business Continuity / by ed. L.Bird. BCI. 2013. 116 p.
7) Tipson H.F. Offi cial ISC2 Guide to the CISSP CBK, 4th ed. ICS2. 2009. 968 p.