Государственное бюджетное образовательное учреждение высшего образования
Московской области
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ
имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

КУРСОВАЯ РАБОТА
по Безопасности информационных систем
(наименование учебной дисциплины)

на тему «Разработка элементов системы обеспечения информационной безопасности на примере ООО «МонтажПромСтрой»»

Выполнил(а) студент(ка) 3 курса, группа ИСТ-20-1
(курс, группа)

_____ Хакимов А.В.
(подпись) (Ф. И. О.)

Руководитель _____ ктн., доцент, Баранова О.М.
(подпись) (Ф. И. О.)

Королев 2023

Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

Институт инфокоммуникационных систем и технологий

Кафедра информационной безопасности

УТВЕРЖДАЮ
Заведующий кафедрой

В.Н. Соляной
«____» _____ 2023 г.

ЗАДАНИЕ *ПО КУРСОВОЙ РАБОТЕ*

Обучающемуся (йся) Хакимову Александру Викторовичу
(фамилия, инициалы)
Тема работы: «Разработка элементов системы обеспечения информационной безопасности на примере ООО “МонтажПромСтрой”»
Дата выдачи задания: «11» 05 2023 г. (день издания приказа)

Срок сдачи законченной работы: 14.06.2023
(в день защиты курсовой работы по расписанию)

Исходные данные курсовой работе: Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", иные законодательные и нормативные акты РФ в области обеспечения информационной безопасности, организационная и функциональная структура организации
Перечень подлежащих разработке вопросов: анализ организационной и функциональной структуры организации, анализ угроз информационной безопасности, определение уязвимостей, анализ информационных рисков, разработка Политики безопасности, разработка мер процедурного (организационного) уровня, разработка мер программно-технического уровня
Перечень графического материала

Руководитель: к.т.н., доцент _____ О.М. Баранова

Задание принял к исполнению _____ Хакимов А.В.
(подпись) (инициалы и фамилия обучающегося)
«12» 05 2023 г.

Оглавление

Введение

Проблема безопасности занимает в современном мире одну из самых серьезных позиций, являясь глобальной проблемой современности.

Безопасность можно рассматривать в разных сферах жизнедеятельности человека, но, как бы то ни было, в любой сфере, где человек вступает в контакт с техникой или другим человеком и группой людей, возникают определенные риски. Современные компьютерные технологии активно внедряются в разные сферы нашей жизни, их применение становится неотъемлемым условием успешной работы.

Любые информационные процессы включают в себя процедуры регистрации, сбора, передачи, хранения, обработки, выдачи информации.

Строительная компания «МонтажПромСтрой» основана в 1999 году и оказывает услуги по строительству, реконструкции, ремонту и проектированию зданий и сооружений любой степени сложности.

Имеет собственное производство по изготовлению стальных и алюминиевых конструкций, изделий из дерева и ПВХ и систем вентиляции. Оказывает услуги по выполнению функций генерального подрядчика и осуществлению функций заказчика-застройщика.

В деятельности современных строительных организаций информационные технологии играют значительную роль, способствуя повышению производительности труда и улучшению качества принимаемых решений. Разработано большое число программных систем, используемых на различных стадиях строительного процесса, в организациях, представляющие разные звенья договорных отношений, специалистами различного профиля.

Обеспечение защиты информации в компании является непрерывным процессом, который предусматривает применение современных методов,

позволяющих вести контроль внешней и внутренней среды предприятия, организацию и реализацию мероприятий по поддержке стабильного функционирования локальной сети и вычислительной техники, а также минимизацию потерь в связи с утечкой информации. Для осуществления защиты информации, как в сетях, так и на производстве, на предприятиях должен быть сформирован определенный свод правил и нормативных документов, регламентирующих действия сотрудников по обеспечению безопасности и описывающий технические и программные средства для защиты информации. Данный свод документов называется политикой информационной безопасности.

Цель выполнения курсовой работы: на основе проведенного анализа организации разработать элементы системы обеспечения информационной безопасности

Задачи, которые должны быть выполнены в ходе курсовой работы:

1. Провести анализ структуры конкретной организации, определить угрозы информационной безопасности и информационные риски

2. Разработать Политику информационной безопасности для конкретной организации

3. Разработать совокупность мер защиты информации на процедурном (организационном) и программно-техническом уровнях

1. Анализ исходной информации

1.1 Анализ организационной и функциональной структуры организации

Важной частью системы анализа деятельности является характеристика организационной и функциональной структуры. В нашем случае организационная и функциональная структуры организации ООО «МонтажПромСтрой» построены с акцентом на предоставление строительных услуг.

Под структурой строительной организации, как и структурой любой другой компании, понимается упорядоченная модель построения подразделений, распределение функций, уровни подчинения, отношения между руководителями и сотрудниками. Структурный подход обеспечивает функционирование и развитие строительной фирмы как целого.

Под структурой строительной организации, как и структурой любой другой компании, понимается упорядоченная модель построения подразделений, распределение функций, уровни подчинения, отношения между руководителями и сотрудниками. Структурный подход обеспечивает функционирование и развитие строительной фирмы как целого.

Общая характеристика предприятия

ООО «МонтажПромСтрой» — активно развивающаяся компания на Российском рынке строительной индустрии. Год основания – 2009. Компания занимается производством элементов инженерных систем и монтажом инженерных сетей.

Описание:

Строительные работы (мелкий текущий ремонт, отделка фасадов, благоустройство территорий, земляные работы и т.д.)

Цель организации - получение прибыли за счет производства и оказания услуг монтажа инженерных систем

Основной вид деятельности:

-производство отделочных работ,

-монтаж инженерного оборудования зданий и сооружений,

-торговля лесоматериалами, строительными материалами и санитарно-техническим оборудованием,

-также осуществление других работ и оказание других услуг.

На предприятии установлена линейно-функциональная организационная структура управления, которая состоит из:

- линейных подразделений, осуществляющих в организации основную работу;

- специализированных обслуживающих функциональных подразделений.

Линейно-функциональная структура управления обладает целым рядом преимуществ:

- быстрое осуществление действий по распоряжениям и указаниям, отдающимся вышестоящими руководителями нижестоящим,

- рациональное сочетание линейных и функциональных взаимосвязей;

- стабильность полномочий и ответственности за персоналом.

- единство и четкость распорядительства;

Краткое описание функций, выполняемых отделами организации:

1. Материально техническое снабжение

2. Производственно-Технический отдел

3. Отдел главного механика

4. Отдел главного электрика

5. Финансовый отдел

6. Отдел сбыта

8. Управление персоналом, в том числе работа с договорами

9. Отдел маркетинга

Линейно-функциональная структура управления ООО «МонтажПромСтрой» показана на рисунке 1.

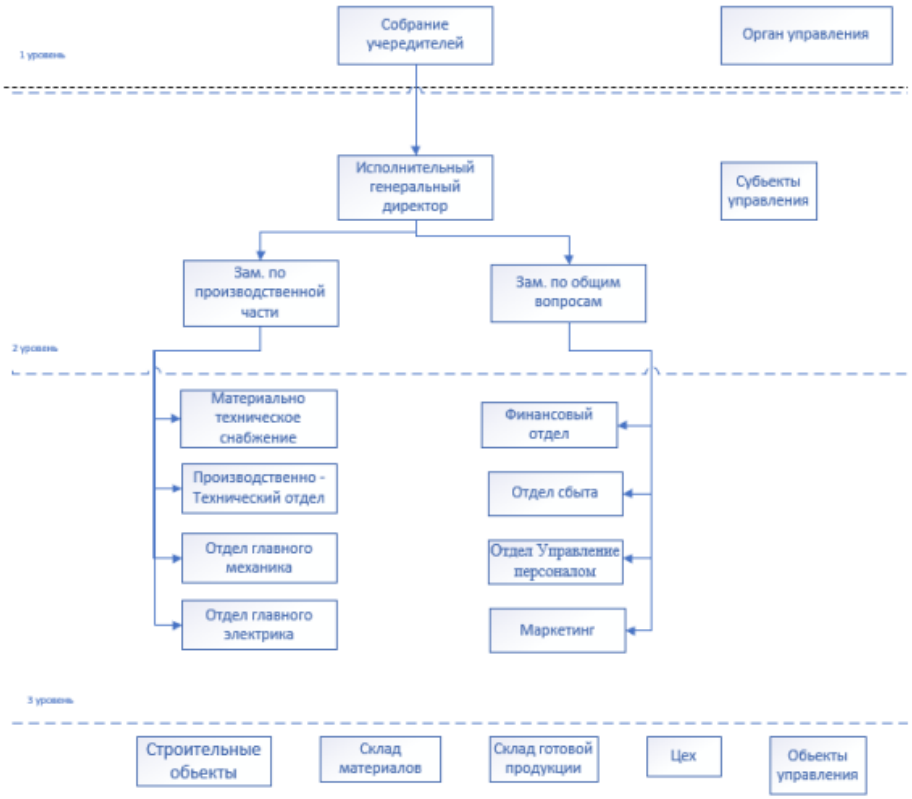

Рисунок 1 – Линейно-функциональная структура

1.2 Анализ угроз информационной безопасности, определение уязвимостей

Основной целью защиты информации является обеспечение заданного уровня ее безопасности. Под заданным уровнем безопасности информации понимается такое состояние защищенности информации от угроз, при которых обеспечивается допустимый риск ее уничтожения, изменения и хищения. При этом под уничтожением информации понимается не только ее физическое уничтожение, но и стойкое блокирование санкционированного доступа к ней. В общем случае при блокировке информации в результате неисправности замка или утери ключа сейфа, забытия пароля компьютера, искажения кода загрузочного сектора винчестера или дискетки и других факторах информация не искажается и не похищается и при определенных усилиях доступ к ней может быть восстановлен. Следовательно, блокирование информации прямой угрозы ее безопасности не создает. Однако при невозможности доступа к ней в нужный момент ее пользователь теряет информацию так же, как если бы она была уничтожена.

Источником опасности могут быть как искусственные, так и естественные угрозы. Искусственные угрозы представляют собой умышленное причинение вреда, а естественные возникают в результате обстоятельств непреодолимой силы, при отсутствии умышленного мотива человека.

К искусственным источникам опасности традиционно относят две группы:

Первая группа:

1. Конкуренты
2. Инсайдеры (внедренные сотрудники)
3. Криминальные организации

4. Хакеры

Вторая группа:

1. Ошибки пользователей
2. Отключение или ошибки в системе безопасности
3. Ошибки в обработке информации
4. Нелицензионное ПО

Естественные источники имеют множество классификаций, к ним относятся любые опасности, которые не зависят от человека.

В данной организации, ООО «МонтажПромСтрой» мною были определены следующие категории информационной безопасности и угрозы:

1. Угрозы в части управления персоналом
    a. Угрозы при увольнении работников
    b. Угрозы при устройстве на работу
    c. Угрозы при отборе соискателей
2. Угрозы в части данных
    a. Утечка данных
    b. Потеря данных
    c. Уничтожение данных
3. Угрозы в части работоспособности ИС
    a. Компьютерные вирусы
    b. Физическое воздействие на аппаратуру
    c. Ошибки пользователей
    d. Отказы и сбои в аппаратуре

1.3 Анализ информационных рисков

Оценка угроз безопасности информации проводится в целях определения угроз безопасности информации, реализация которых возможна в системах и сетях с заданной архитектурой и в условиях их функционирования - актуальных угроз безопасности информации.

Разбор рисков информационной безопасности дает возможность определять критические факторы, оказывающие отрицательное влияние на бизнес-процессы предприятия, и принимать меры для их предотвращения или минимизация негативного воздействия.

Необходимо понимать, на какой стадии находится информационная система организации, она обязана отвечать установленному комплексу требований к обеспечению информационной безопасности.

Основными задачами, решаемыми в ходе оценки угроз безопасности информации, являются:

1. оценка реализации угроз безопасности информации в системах
2. оценка возникновения угроз
3. определение негативных последствий от угроз безопасности информации

На этапе создания систем и сетей результаты оценки угроз безопасности информации должны быть направлены на обоснование выбора организационных и технических мер по защите информации, а также на выбор средств защиты информации и их функциональных возможностей.

На основе анализа информационной системы ООО «МонтажПромСтрой» были определены следующие защищаемые активы:

1. Базы данных компании
2. Персональные данные клиентов, поставщиков и т.д.
3. Сервера компании
4. Программное обеспечение компании

В ходе оценки угроз безопасности информации были определены негативные последствия, по защищаемым активам, которые могут наступить от возникновения угроз безопасности информации:

1. Базы данных компании
    a. Уничтожение информации
    b. Утечка информации
2. Персональные данные клиентов, поставщиков и т.д.
    a. Утечка персональных данных
3. Сервера компании
    a. Намеренная порча оборудования (физическая)
    b. Заражение и выведение из строя вирусами.
4. Программное обеспечение компании
    a. Использование ломанного (нелицензионного ПО)
    b. Внедрение вирусов

Анализ статистики происшествий.

ООО «МонтажПромСтрой» не имеет собственного веб-сайта. Статистика происшествий была определена из анализа происшествий из аналогичных компаний. Статистика является неточной, но приближена к реальности.

1. Базы данных компаний в сфере строительства имеют хорошую защищенной от внешних и внутренних угроз, так как данные компании в большинстве случаев используют существующие Системы Управлений Базами Данных, которые включают в себя обширную систему разграничения доступа, управление ролями и др.
    a. Уничтожение информации может нанести компании серьезный ущерб, но в современном мире компании используют периодичное резервное копирование, которое предотвращает полное удаление информации. Исходя из этого, база данных организации защищена от данной угрозы на 94%
    b. Утечка информации, в отличие от уничтожения, не полностью защищена. При утечке информации данные могут попасть в руки злоумышленника, после чего, дальнейшее распространение информации невозможно предотвратить. Утечка информации может произойти в случае ее копирования или переписывания лицом внутри компании, заражения сервера или программного обеспечения и т.д. Организация защищена от данной угрозы на 23%
2. Персональные данные клиентов, поставщиков и т.д. зачастую хранятся в базе данных, но в редких случаях они могут храниться на облачном хранилище в виде документов. Персональные данные являются важной частью документ-обеспечения компании.
    a. Утечка персональных данных является частым происшествием в организациях. Происходит утечка персональных данных в разных случаях, таких как: кража данных с сервера «подсадными» людьми, взлом информационной системы или несанкционированный вход в систему и т.д. Компания защищена от данной угрозы на 78%

3. Сервера компании зачастую являются облачными, но в некоторых случаях они являются физически-доступными в условном офисе компании. Доступ к такому серверу осуществляется с помощью прокси или VPN. Физически-доступные сервера имеют повышенную опасность для негативных последствий.
    a. Физическая порча оборудования возможна только случае существования подельника в компании, у которого есть определенный уровень доступа. Так как серверная в большинстве случаев имеет элементы системы безопасности, при которых необходимо иметь ключ или код, для доступа к серверной, то пробраться внутрь может только сотрудник с доступом к ней. Компания защищена от данной угрозы на 96%
    b. Заражение и выведение из строя сервера путем заражения последнего, так же сложно, так как серверная часть информационной системы не имеет возможности запускать и хранить исполняемые файлы, которые были получены извне. Заражение может быть произведено, если физически подключить флеш-карту или ноутбук к серверу. Данная угроза в большинстве случаев является наименее опасной, но, все-таки есть случаи заражения серверов, которые были недостаточно защищены. Компания защищена от данной угрозы на 88%.
4. Программное обеспечение компании может включать в себя как офисные программы, так и инженерные программы, административные программы и т.д. Заражение ПО может повлечь за собой большие потери компании.
    a. Использование инженерного нелицензионного ПО в компании ООО «МонтажПромСтрой» может привести к неточным расчетам программы, сбоям в работе при создании конструкций и т.д. Использование нелицензионного ПО также может привести к заражению ПК пользователей. Поэтому, для

предотвращения этой угрозы необходимо использовать лицензионное ПО.

Для оценки рисков информационных угроз был выбран метод FRAP.

Определение вероятности возникновения угроз, оценка ущерба, который может быть нанесен данной угрозой, оценка уровня угрозы, исходя из полученных значений.

Ниже приведена таблица 1 уровней риска в отношении Степень воздействия на бизнес/Уровень уязвимости

		Степень воздействия на бизнес		
		Высокая	Средняя	Низкая
Уровень уязвимости	Высокий	A	B	C
	Средний	B	B	C
	Низкий	C	C	D

Таблица 1 – Таблица уровней риска

Классификация приведенных угроз в сопоставлении с таблицей:

1. Базы данных компании
    a. Уничтожение информации - B
    b. Утечка информации - A
2. Персональные данные клиентов, поставщиков и т.д.
    a. Утечка персональных данных - B
3. Сервера компании
    a. Намеренная порча оборудования (физическая) - A
    b. Заражение и выведение из строя вирусами. - A
4. Программное обеспечение компании
    a. Использование ломанного (нелицензионного ПО) - B
    b. Внедрение вирусов - B

2. Разработка Политики безопасности

Политика информационной безопасности представляет собой систематизированное изложение целей и задач защиты, правил и практических приемов в области информационной безопасности.

Основными объектами системы информационной безопасности в компании являются:

- информационные ресурсы, необходимые для работы
- информационные технологии и процедуры сбора, обработки, хранения и передачи информации, разработчики, пользователи системы и обслуживающий персонал
- информационная структура, включающая системы обработки и анализа информации, программные средства ее обработки, передачи и отображения, в том числе системы и средства защиты информации

Стоит отметить, что политики безопасности может нанести значительный ущерб. Законодательство Российской Федерации выделяет несколько видов массивов защищаемой информации, доступ к работе, с которой имеют предприятия различной формы собственности и государственные органы:

1. коммерческая тайна
2. государственная тайна, к которой могут получить многие участники тендеров на гос. закупки
3. персональные данные сотрудников и других лиц

Утечка этих данных с использованием любых каналов незаконного перехвата информации может привести к ухудшению деловой репутации компании, отзыву лицензии или иного доступа к данным, которые охраняются особым образом, потере клиентов и т.д.

Основной целью политики информационной безопасности является защита информационных субъектов от возможного нанесения им материального, физического или иного ущерба, посредством преднамеренного воздействия на информацию, процессы обработки и передачи.

Кроме того, целями информационной безопасности компании являются:

- защита конфиденциальности информации клиентов и сотрудников
- защита экономических данных компании
- защита имущества предприятия

Для достижения основной цели обеспечения информационной безопасности необходимо решить следующие задачи:

- своевременное выявление, оценка и прогнозирование угроз информационной безопасности, причин и условий, способствующих нанесению ущерба
- создание оперативного реагирования на угрозы безопасности информации
- создание условий для минимизации наносимого ущерба
- разграничение доступа пользователей
- обеспечение аутентификации пользователей
- защиту от несанкционированной модификации используемых программных средств
- обеспечение криптографических средств защиты информации.

Решение обозначенных задач может быть достигнуто:

- учетом всех подлежащих защите ресурсов
- учет всех действий сотрудников
- разграничением прав доступа к ресурсам
- соблюдением всеми сотрудниками требований документов по обеспечению безопасности информационной системы

- применение средств защиты ресурсов системы и непрерывная поддержка

Исходя из вышеперечисленного, политика безопасности для компании ООО «МонтажПромСтрой» имеет вид:

1. Общие положения:

- Компания строго соблюдает законы, правила и регуляции относительно защиты информации и данных.

- Компания устанавливает полную ответственность на своих сотрудников за нарушение политики безопасности.

- Компания обеспечивает техническую и меры безопасности рабочей среды для защиты от внешних и внутренних угроз.

2. Управление доступом:

- Все новые члены персонала должны проходить обучение по политике безопасности компании и дать согласие на ее соблюдение.

- Все пользователи должны иметь уникальные идентификаторы и пароли для доступа к компьютерным системам компании.

- Доступ должен быть предоставлен только в меру необходимости для исполнения рабочих обязанностей.

- Доступ к чувствительной информации, такой как данные об оплате, может быть предоставлен только определенным сотрудникам, назначенным менеджерами.

3. Обработка данных:

- Все компьютеры и сервера компании должны быть защищены от вирусов и вредоносного ПО путем установки соответствующего программного обеспечения и периодической проверки систем на наличие угроз.

- Вся информация должна регулярно резервироваться и копироваться для предотвращения потери данных.

- На все узлы сети должен быть установлен механизм автоматического блокирования аккаунтов при определенном количестве неверных попыток входа в систему.

4. Физическая безопасность:

- Компания ограничивает доступ к компьютерным системам и серверам только для уполномоченного персонала.

- Компания должна держать свои здания в безопасном состоянии, обеспечивать контроль доступа и соответствующую идентификацию при проведении работ внутри офиса и на строительных площадках.

- Физические копии документов должны храниться в местах с ограниченным доступом.

Данная политика распространяется на всех сотрудников предприятия и требует полного подчинения. Данная политика укрепляет общую политику безопасности компании. Весь персонал должен быть ознакомлен и ответственен за информационную безопасность в рамках своих полномочий.

Генеральный директор отвечает за обеспечение проработки информации во всей организации. Каждый начальник отдела отвечает за то, чтобы сотрудники, работающие под его руководством, осуществляли защиту информации. Каждый сотрудник организации отвечает за информационную безопасность.

Таким образом, определены основные задачи по организации политики информационной безопасности в ООО «МонтажПромСтрой» и пути их решения.

3. Разработка мер обеспечения информационной безопасности

3.1 Разработка мер процедурного (организационного) уровня

Теперь мы должны рассмотреть меры безопасности, которые ориентируются на людей. Люди формируют режим информационной безопасности, и они же оказываются одной из главных угроз, поэтому человеческий фактор необходимо принимать во внимание, при определении мер безопасности.

Следует осознать степень зависимости от компьютерной обработки данных, в которую попало современное общество. Без преувеличения можно сказать, что необходима информационная «оборона».

Процедурный уровень, это меры безопасности, реализуемые людьми, программно-технический уровень - непосредственно средства защиты информации. Законодательный уровень является основой для построения системы защиты информации, так как дает базовые понятия предметной области и определяет меру наказания для потенциальных злоумышленников.

К процедурному уровню относятся меры безопасности, реализуемые сотрудниками предприятия. Выделяются следующие группы процедурных мер, направленных на обеспечение информационной безопасности:

- управление персоналом
- физическая защита
- поддержание работоспособности
- реагирование на нарушения режима безопасности
- планирование восстановительных работ

При определении мер обеспечения информационной безопасности процедурного уровня следует определить и проанализировать угрозы информационного уровня, при котором человек является основной «отправной точкой» угрозы.

Из всех определенный ранее угроз, которые подходят под процедурный уровень обеспечения процедурного уровня безопасности можно выделить:

1. Уничтожение информации
2. Утечка информации
3. Утечка персональных данных
4. Заражение и выведение из строя вирусами.
5. Использование ломанного (нелицензионного ПО)

Каждый из перечисленных угроз от части зависят от поведения человека, его отношения к информационной безопасности и человеческого фактора.

Ниже будут перечислены примеры решений угроз:

1. Составление правил и режима проверки и обработки написанных программ и кодов, направленных на обеспечение информационной целостности и безопасности информационной системы. Проверка системой безопасности исполнение данных правил и режима. Ежедневная проверка дневника, который должен быть создан для отчетности проверок системы.
2. Обучение сотрудников: обучение персонала компании основам безопасности информации, регулярное проведения аудитов безопасности и обновления списков контроля доступа.
3. Профилактические работы и тестирование сети и системы на поиски угроз и потенциальных «щелей» в системе. Также, как и в первом пункте, данные работы должны проводиться периодично с проверкой вышестоящих лиц отдела безопасности.

4. Блокировка и контролирование трафика персонала. Вся информация, просматриваемая и скачиваемая из открытого доступа, должна проверяться автоматизированными системами безопасности, установленных на персональных компьютерах сотрудников. Этими системами могут быть лицензионные проверенные антивирусы, или собственно-разработанные системы безопасности, которые будут проверять все скачанные файлы и непроверенные сайты, которые посещают сотрудники, с их последующей блокировкой.

5. Проведение повышения квалификации для работников отдела информационной безопасности. Данное предложение позволит повысить профессиональные знания и навыки для дальнейшего пресечения потенциальных угроз информационной системы.

6. Должна осуществляться полная проверка человека, которого принимают на работу. Информация может включать в себя: предыдущее место работы, родственники и их места работы, возможные связи с компаниями конкурентов, судимости и др. Полученная информация даст возможность отсеивать неподходящие кадры, для предотвращения угрозы в будущем.

7. Разработка ролевой модели доступа. Каждый сотрудник должен иметь определенную роль и режим доступа к важным объектам информационной системы компании. Разработкой ролевой модели должны заниматься разработчики совместно с отделом информационной безопасности. Данное решение предотвратит угрозу несанкционированного доступа к информационной системе людьми, которые не должны иметь доступ к определенным блокам последней.

3.2 Разработка мер программно-технического уровня

Программно-технические меры, т. е. меры, направленные на контроль компьютерных сущностей — оборудования, программ, данных. Ущерб наносят в основном действия пользователей, по отношению к которым процедурные регуляторы неэффективно. Только программно-технические меры способны противостоять некомпетентности сотрудников.

Типовые системы защиты информации:

- Типовая система защиты от несанкционированного доступа
- Типовая система защиты от угроз вредоносного кода
- Типовая система анализа защищенности
- Типовая система обнаружения вторжения
- Типовая система мониторинга событий безопасности

1. Использование периодичного резервного копирования информации. Резервное копирование, это процесс создания копии данных на носителе, предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения. При возможном происшествии, при котором будет уничтожена информация, будет возможность ее восстановления, что предотвращает возможность полного исчезновения информации. Резервное копирование, в зависимости от важности и количества информации может быть выполнено по расписанию или физически оператором баз данных в определенные прописанные промежутки времени. Так как информация, находящаяся в базе данных нашей компании, является особо важной, так как представляет из себя

персональные данные, данные клиентов, заказчиков, поставщиков, то резервное копирование должно производиться раз в день-два.

2. Шифрование и кодирование информации. При утечке данных, происходит копирование информации из баз данных. Если информация, находящаяся в базе данных, будет представления в простом виде, то утечка данных приведет к немедленному ее распространению, однако, использование шифрования информации дает возможность хранить информацию в базе данных в виде определенного набора хаотично расположенных символов, которые могут быть правильно прочитаны только дешифратором, который может представлять из себя лицензионным программным обеспечением, или собственно разработанным программным продуктом. Все это, позволяет компании, даже в случае утечки информации, не волноваться на счет украденной информации, а заниматься усовершенствованием системы безопасности. Шифрование данных в сети Интернет производиться с использованием компанией сертификатов шифрования данных HTTPS и сертификатами безопасности SSL/TLS. На стороне обработчиков и сервера должны быть организованы системы шифрования данных при попадании и выборке данных из БД, например AES.

3. Антивирусное программное обеспечение и защита от вредоносных программ: компания должна иметь установленное антивирусное программное обеспечение и систему защиты от вредоносного ПО, которая регулярно обновляется, чтобы защитить от новых угроз. Самым популярным и сильным антивирусным ПО для бизнеса и мультипользовательского использования является Cisco Secure Endpoint Essentials. Обширные настройки, обработка сценариев, проработанная защита от угроз и огромный черный список дает возможность сильно снизить риски взаимодействия вирусов на ПК пользователей и сервер.

4. Управление доступом и идентификация пользователей: компания должна обеспечить управление доступом и идентификацию пользователей, чтобы обеспечить защиту от несанкционированного доступа. Операционная система для сервера - Windows Server, дает гибкую настройку ролевой модели пользователей сервера, обширную настройку политики безопасности, блокировку входящего трафика и многое другое. Если в компании используется 1С, то управление личными кабинетами пользователей системой производится администраторами. Доступ к базе данных так же настраивается администратором базы данных, создание ролевой модели и распределение доступа позволит защитить данные от удаления, изменения и копирования.

5. Установка программного обеспечения, проведение обслуживания и обновлений: все программное обеспечение должно устанавливаться только из надежных источников, а все регулярные обновления и патчи должны быть установлены без задержек. Использование Kaspersky Internet Security позволит решить две проблемы сразу, программа защитит от сетевых и вирусных угроз, а также позволит в реальном времени оповещать системного администратора о возможности обновления того или иного приложения, таким образом программное обеспечение всегда будет свежей версии, и скачано с официальных ресурсов, что предотвратит возможность установки некачественного ПО.

6. Сетевая безопасность: компания должна обеспечить сетевую безопасность, чтобы обеспечить защиту от атак и утечек данных. Наличие сильного Firewall может обеспечить pfSense. Помимо Firewall, pfSense дает серверную балансировку нагрузки, VPN, динамический DNS. Использование VPN дает возможность туннелировать трафик, поступающий или исходящий на сервер, перехват таких сигналов почти невозможен. Переход с HTTP на HTTPS позволит шифровать данные и

усилит безопасность передачи данных. Использование протокола SSH также увеличит защищенность данных при передаче. Использование удаленного доступа RDP и четкая настройка учетных записей и точки входа на сервер. При полной настройке групп и пользователей, а также политики безопасности доступа на сервер, угрозы проникновения и уничтожение данных могут быть сведены на нет.

Эти меры безопасности помогут защитить компанию от множества угроз и обеспечат сохранность её данных и конфиденциальности.

4. Выводы

В результате выполнения курсовой работы на тему «Разработка элементов системы обеспечения информационной безопасности ООО «МонтажПромСтрой»» была разработана политика безопасности, охватывающая ключевые аспекты защиты информации и данных компании. Также проведен анализ структуры организации, угрозы информационной безопасности и информационных рисков. Было установлено, что защита информации в строительных компаниях имеет высокую важность, так как на ее основе принимаются стратегические решения и осуществляется управление проектами.

Разработка мер процедурного уровня, а также мер программно-технического уровня дала возможность определить возможные угрозы, меры их решения и предостережения от них.

Основное внимание было уделено управлению доступом к чувствительной информации, обеспечению обработки и хранения данных, защите компьютерной среды от вредоносных программ и осуществлению надежной аутентификации сотрудников.

В целом, курсовая работа была успешно выполнена и политика безопасности, разработанная в результате ее выполнения, должна служить инструментом защиты информационной сети строительной компании от угроз и уязвимостей, гарантируя надежность и конфиденциальность данных, оптимизацию процессов управления и увеличение эффективности бизнес-операций компании.

5. Список литературы

1. Осовецкий Леонид Георгиевич, Суханов Андрей Вячеславович, Ефимов Вячеслав Викторович Меры по обеспечению безопасности и защиты информации для сложных информационных систем // Системы управления, связи и безопасности. 2017. №1. URL: https://cyberleninka.ru/article/n/mery-po-obespecheniyu-bezopasnosti-i-zaschity-informatsii-dlya-slozhnyh-informatsionnyh-sistem (дата обращения: 24.05.2023).
2. Манжуева Оксана Михайловна, Костылева Ольга Петровна Краткий анализ основных мер обеспечения информационной безопасности // Евразийский Союз Ученых. 2018. №6 (51). URL: https://cyberleninka.ru/article/n/kratkiy-analiz-osnovnyh-mer-obespecheniya-informatsionnoy-bezopasnosti (дата обращения: 24.05.2023).
3. ГОСТ Р ИСО/МЭК 27000—2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»
4. ГОСТ Р ИСО/МЭК 15408-2-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности»
5. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»
6. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»

7. Язовский А. М., Шабурова А. В., Гавриленко Н. Л. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ // Интерэкспо Гео-Сибирь. 2022. №. URL: https://cyberleninka.ru/article/n/politika-informatsionnoy-bezopasnosti-v-organizatsii (дата обращения: 24.05.2023).
8. Тершуков Дмитрий Анатольевич Анализ современных угроз информационной безопасности // NBI-technologies. 2018. №3. URL: https://cyberleninka.ru/article/n/analiz-sovremennyh-ugroz-informatsionnoy-bezopasnosti (дата обращения: 24.05.2023).
9. Горохов Г.В. «Информационная безопасность предприятия», СПб: Издательский дом «Питер», 2016.