Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования «Национальный исследовательский университет
ИТМО»

Факультет инфокоммуникационных технологий

Основы кибербезопасности

Практическая работа №2

Выполнил:

студент группы K34211

Швалов Даниил Андреевич

Проверил:

преподаватель практики, КТН

Назаров Михаил Сергеевич

Санкт-Петербург

2024

Оглавление

Введение

Цель работы. Изучить типовой алгоритм описания информационной системы. Приобрести практические навыки по его применению. Научиться идентифицировать угрозы информационной системы, их источники и методы планирования.

Содержание отчета

1. Описание и структура информационного объекта

Информационным объектом для данной практической работы была выбрана коллегия адвокатов — негосударственная, независимая, самоуправляемая и самоконтролируемая организация профессиональных юристов, добровольно объединившихся в целях оказания квалифицированной юридической помощи физическим и юридическим лицам.

Коллегия адвокатов оказывает такие юридические услуги, как:

— проведение консультаций и составление справок по правовым вопросам;

— составление заявлений, жалоб и других документов правового характера;

— представление интересов в судопроизводстве;

— участие в качестве представителя доверителя.

Юридические услуги оказываются на основе гражданско-правового договора между адвокатом и доверителем.

Коллегия адвокатов обладает внутренней структурой, описанной в таблице 1.

Таблица 1 — Должности и обязанности в коллегии адвокатов

Должность	**Обязанности**
Президент коллегии	Организация и планирование работы коллегии, заключение договоров и сделок, распоряжение средствами коллегии, осуществление контроля за работой адвокатов

Президиум коллегии	Руководство деятельности адвокатов и адвокатских консультаций, принятие и исключение из коллегии, поощрение адвокатов, организует проверки работы адвокатов
Совет коллегии	Организация и контроль за качеством работы адвокатов, разработка и принятие внутренних нормативных актов, управление финансами коллегии
Ревизионная комиссия	Ревизии финансово-хозяйственной деятельности коллегии
Технические специалисты	Разработка и поддержка информационно-технической инфраструктуры коллегии

2. Структура и род деятельности информационного объекта

В коллегии адвокатов работают со следующими данными:

— информация о клиенте (ФИО, контактные данные, история обращений и т. п.);

— юридическая информация (документы, справки, выписки, судебное делопроизводство и т. п.);

— административная информация (информация об адвокатах, их ФИО, контактные данные, информация об их рабочей деятельности и т. п.).

Часть из перечисленных данных могут являться конфиденциальными, т. е. у злоумышленников или простых пользователей не должно быть прямого доступа к ним. Поэтому такие данные должны быть защищены должным образом.

3. Описание информационно-технической инфраструктуры информационного объекта

На рисунке 1 приведена схема информационно-технической инфраструктуры рассматриваемой коллегии адвокатов.

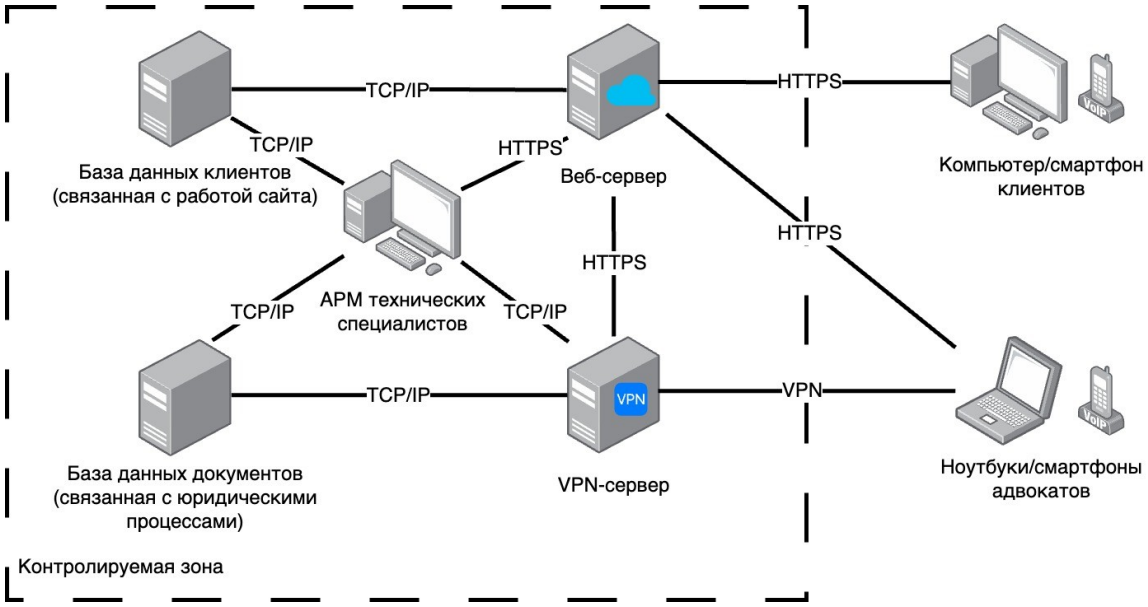

Рисунок 1 — Схема информационно-технической инфраструктуры коллегии адвокатов

Схема информационно-технической инфраструктуры, состоит из следующих компонентов:

— веб-сервера, который обслуживает информационный портал коллегии адвокатов и позволяет клиентам получить информацию или способ связи с коллегией;

— VPN-сервера для безопасного доступа адвокатов в контролируемую зону;

— база данных клиентов, в которой хранятся данные, сохраняемые с веб-сервера (например, записи на прием);

— база данных документов, где хранится различная конфиденциальная информация.

Предполагается, что клиенты могут иметь доступ только к информационному порталу коллегии адвокатов. Для взаимодействия с порталом предлагается использовать протокол HTTPS.

При этом самим адвокатам может понадобиться доступ к различным конфиденциальным документам. Для безопасной передачи данных предлагается использовать собственный VPN-сервер, например, на базе OpenVPN. Это позволит быть уверенным в том, что конфиденциальные данные передаются достаточно защищенно по сети.

Для настройки и поддержки информационно-технической инфраструктуры предлагается использовать автоматизированное рабочее место для технических специалистов, находящееся в контролируемой зоне.

4. Перечень необходимого оборудования

Для эффективной работы коллегии адвокатов требуется следующее оборудование:

— компьютеры и мобильные устройства для адвокатов (для возможности быстро получить или передать информацию);

— серверное оборудование (для веб-сервера, VPN-сервера и баз данных);

— сетевое оборудование для организации внутренней сети (например, маршрутизаторы, коммутаторы, беспроводные точки доступа и т. п.);

Кроме технических средств, коллегия адвокатов также имеет дело с большим количеством бумажной работы. Поэтому коллегия адвокатов должна быть обеспечена всем необходимым для удобной и эффективной работы с бумажными документами, например:

— удобные кресла и письменные столы для возможности комфортно работать продолжительное количество времени;

— необходимые письменные принадлежности (например, бумага, ручки, печати и чернила, папки и файлы);

— принтеры и сканеры.

При необходимости адвокатов можно обеспечить местом для проведения обеденного перерыва. Для этого могут потребоваться следующее оборудование:

— микроволновая печь;

— холодильник;

— кофемашина;

— чайник;

— тарелки и столовые приборы;

— кружки.

5. Перечень активов информационного объекта

Коллегия адвокатов обладает обширным перечнем информационных активов. Основная часть из них приведена в таблице 2.

Таблица 2 — Перечень активов информационного объекта

Тип актива	**Свойства информационного актива**			**Стоимость актива**
	целостность	**доступность**	**конфиденциальность**	
Информация о клиентской базе: ФИО, персональная информация и прочие данные	+	+	+	20000
Юридические конфиденциальные документы	+	+	+	20000
Годовые финансовые отчеты работы коллегии	+	+	+	20000
Персональная информация об адвокатах	+	+	+	20000

Публичная информация о коллегии с информационного портала	+	+	-	5500
Данные о рабочем оборудовании, выданном адвокатам	+	-	+	5000
Данные об оборудовании и устройстве внутренней инфраструктуры	+	-	-	5000
Данные о наличии расходных бумажных материалов	-	-	-	500
Данные о бытовой технике, числящейся в коллегии	-	-	-	500

Согласно таблице 2, общая стоимость всех информационных активов составляет 96500 у.е.

6. Определение угроз, их источников и методов борьбы с данными угрозами

Для коллегии адвокатов были определены различные источники угроз и методы борьбы с ними. Они приведены в таблице 3.

Таблица 3 — Определение угроз, их источников и методов борьбы с данными угрозами

Уязвимость	**Название угрозы**	**Источник угрозы**	**Последствия реализации угрозы**	**Методы борьбы**
Слабое понимание принципов информационной защиты сотрудниками	Фишинг	Злоумышленники, киберпреступники	Утечка конфиденциальной информации	Обучение сотрудников, многофакторная аутентификация, использование антивирусов
Небезопасное использование инструментов удаленного доступа	Удаленное управление скомпрометированным устройством	Злоумышленники, киберпреступники	Утечка конфидециальной информации, установка бэкдоров, компрометация внутренней инфраструктуры	Обучение сотрудников, ограничение на использование инструментов удаленного доступа
Отсутствие защитных средств от перегрузки системы злоумышленниками	Распределенный отказ в обслуживании	Злоумышленники, киберпреступники	Невозможность оказания услуг, потеря клиентов	Использование технических средств противодействия
Использование незащищенного канала передачи данных	Сетевой сниффинг	Злоумышленники, киберпреступники	Утечка конфиденциальной информации	Использование защищенных каналов передачи данных

Хранение секретов в незащищенном виде	Компрометация секретов	Злоумышленники, киберпреступники	Утечка конфиденциальной информации, компрометация внутренней инфраструктуры	Хранение секретов в защищенном виде, разграничение доступов
Небезопасная работа с входными пользовательскими данными	Инъекция исполняемого кода	Злоумышленники, киберпреступники	Утечка конфидециальной информации, установка бэкдоров, компрометация внутренней инфраструктуры	Использование средств обработки и фильтрации входных пользовательских данных

Вывод по работе

В результате выполнения данной практической работы был изучен и применен типовой алгоритм описания информационной системы, получен опыт идентификации угроз информационной системы, их источников и методов планирования.