|  |  |
| --- | --- |
| **лого для документов 2022** | ***Федеральное агентство по рыболовству***  ***Федеральное государственное бюджетное образовательное***  ***учреждение высшего образования***  ***«Астраханский государственный технический университет»***  **Система менеджмента качества в области образования, воспитания, науки и инноваций**  **ООО «ДКС РУС» по международному стандарту ISO 9001:2015** |

ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ

**КАФЕДРА АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ И УПРАВЛЕНИЯ**

**ОРГАНИЗАЦИОННЫЕ МЕТОДЫ**

**ЗАЩИТЫ ИНФОРМАЦИИ**

(*наименование дисциплины*)

**ОТЧЕТ**

о выполнении заданий к лабораторной работе №3

**«ПРАВОВЫЕ НОРМЫ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ»**

*(название лабораторной работы)*

|  |  |
| --- | --- |
|  | Выполнила:  студент гр. ДИНРБ-41 |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Кузургалиев Р.А. |
|  | «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_2024 г. |
|  | Максимальное количеству баллов \_\_\_\_\_  ЗАЩИЩЕНО:  Получено баллов \_\_\_\_\_\_ |
|  | Преподаватель: \_\_\_\_\_\_\_Сахипова Ж.Ш. |
|  | «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_2024 г. |

**Астрахань – 2024**

**Лабораторная работа №3 «ПРАВОВЫЕ НОРМЫ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ»:**

**Задание**

1. Оцените угрозы вашим информационным ресурсам (укажите наиболее вероятные виды компьютерных преступлений).
2. Укажите мероприятия, проводимые при создании системы защиты информации в вашей компьютерной сети.
3. Укажите перечень РД ГТК, учитываемых при разработке «Политики безопасности» на вашем предприятии.
4. Определите и обоснуйте требования по защите вашей конфиденциальной информации – группу и класс защищенности СВТ от НСД (с использованием РД ГТК).

**Ход работы:**

Название: "ИнноваТек"

Вид деятельности: Разработка программного обеспечения

Область деятельности: IT-услуги для бизнеса, включая создание программного обеспечения на заказ и хранилище данных.

1. Оценка угроз информационным ресурсам

Наиболее вероятные виды компьютерных преступлений для компании "ИнноваТек":

* Малварь: Вредоносные программы, такие как ransomware, могут зашифровать данные и требовать выкуп.
* Фишинг: Мошеннические попытки получить конфиденциальные данные сотрудников или клиентов.
* Неавторизованный доступ: Попытки взлома систем для получения доступа к данным.
* Утечка данных: Неправомерное распространение конфиденциальной информации.
* DDoS-атаки: Сетевые атаки, направленные на перегрузку серверов и доступность услуг.

2. Мероприятия по созданию системы защиты информации

При создании системы защиты информации в компьютерной сети можно провести следующие мероприятия:

* Аудит безопасности: Анализ текущих систем безопасности и выявление уязвимостей.
* Шифрование данных: Использование криптографических средств для защиты данных при передаче и хранении.
* Фаерволы и системы предотвращения вторжений: Настройка защиты на границе сети.
* Обучение сотрудников: Проведение тренингов по кибербезопасности и политике безопасности компании.
* Регулярное обновление ПО: Установка обновлений для устранения уязвимостей в программном обеспечении.

3. Перечень РД ГТК для разработки «Политики безопасности»

При разработке «Политики безопасности» в "ИнноваТек" следует учесть следующие РД ГТК (регулирующие документы государственной технической комиссии):

* ФЗ-152 "О персональных данных": Нормативные требования к обработке и защите персональных данных.
* ФЗ-149 "Об информации, информационных технологиях и защите информации": Общие нормы регулирования в сфере информации.
* Методические рекомендации по оценке защищенности информационных систем: Установление критериев для оценки рисков и уязвимостей.
* Регламенты и стандарты ИТ-сферы: Например, стандарты ISO/IEC 27001 по управлению информационной безопасностью.

4. Требования по защите конфиденциальной информации

* Группа и класс защищенности системы обработки данных от несанкционированного доступа (НСД):
* Группа защищенности: Информация о клиентах, финансовые данные, технологии разработки ПО относятся к группе конфиденциальной информации.
* Класс защищенности: На основании оценки рисков можно определить, что для крепкой защиты требуется не менее III класса защищенности, что подразумевает использование комплексных мер защиты (шифрование, многоуровневая аутентификация и т.д.).

**Контрольные вопросы:**

1. Особенности расследования компьютерных преступлений

* Специфика объектов: Виртуальные объекты и данные, которые могут быть удалены, изменены или зашифрованы.
* Технические трудности: Сложность в сборе и анализе улик из-за особенностей современных технологий.
* Необходимость в специализированных знаниях: Потребность в экспертах в кибербезопасности для проведения технической экспертизы.
* Глобальность преступлений: Преступления могут осуществляться на международном уровне, что требует сотрудничества с правоохранительными органами других стран.

2. Задачи судебно-бухгалтерской и программно-технической экспертиз

Судебно-бухгалтерская экспертиза:

* Анализ финансовых документов и транзакций.
* Установление факта финансовых злоупотреблений или махинаций.

Программно-техническая экспертиза:

* Оценка технического состояния компьютерных систем.
* Анализ источников данных и цифровых улик (логи, сетевой трафик).
* Восстановление удалённых данных.

3. Существующая классификация компьютерных преступлений

Классификация может включать следующие категории:

* Преступления против конфиденциальности: Неавторизованный доступ к данным (НСД).
* Преступления против целостности: Вредоносные действия, влияющие на целостность данных (например, изменение, удаление).
* Преступления против доступности: DDoS-атаки, которые приводят к недоступности сервисов.
* Преступления против авторских прав: Нарушение прав на программное обеспечение и контент.

4. Методы и приемы предупреждения компьютерных преступлений

* Обучение и повышение осведомленности работников о киберугрозах.
* Использование антивирусного ПО и фаерволов для защиты систем.
* Регулярные аудиты безопасности и тестирование на уязвимости.
* Установление протоколов реагирования на инциденты и мониторинг сетевой активности.
* Анализ компьютерных преступлений: Идентификация уязвимостей и паттернов поведения злоумышленников для улучшения защиты.

5. Нормы правового обеспечения защиты информации в АС

* Федеральный закон "О персональных данных".
* Федеральный закон "Об информации, информационных технологиях и защите информации".
* Постановления и инструкции Федеральной службы безопасности (ФСБ) и других регулирующих органов.

6. Документ «Политика безопасности»

Политика безопасности – это свод правил и процедур, направленных на защиту информации и ресурсов компании. Она включает:

* Определения ролей и обязанностей сотрудников в области информационной безопасности.
* Процедуры обработки, хранения и передачи конфиденциальной информации.
* Механизмы реагирования на инциденты в области безопасности.

7. Документы для присвоения класса защищенности АС

* Документы, подтверждающие идентификацию и классификацию информации.
* Оценка рисков и угроз для автоматизированной системы.
* Технические условия и спецификации на программное и аппаратное обеспечение.

8. Выбор класса защищенности СВТ

Выбор класса защищенности зависит от:

* Значимости обрабатываемой информации.
* Уровня риска для бизнеса и репутации компании.
* Нормативных требований и стандартов безопасности, которым нужно соответствовать.

9. Правила безопасности в «Политике безопасности»

Правила, обеспечиваемые «Политикой безопасности», включают:

* Регламенты по доступу к информации.
* Процедуры реагирования на инциденты.
* Шифрование данных и безопасное хранение информации.
* Обучение и информирование сотрудников.

10. Требования к безопасности компьютерных сетей в РФ

Требования к безопасности компьютерных сетей указаны в следующих документах:

* ФЗ-149 "Об информации, информационных технологиях и защите информации".
* РАСПОРЯЖЕНИЕ Правительства РФ о мерах по обеспечению кибербезопасности.
* Нормативные акты ФСБ и других регулирующих органов по охране информации.

Вывод: В процессе работы над темой освоения методов правовой защиты информации в автоматизированных системах (АС) было выявлено, что комплексный подход к защите информации включает как правовые, так и технические меры.

Правовая защита информации играет ключевую роль в обеспечении безопасности данных, основанной на применении действующего законодательства, разработке внутренних нормативов и процедур, а также внедрении эффективных мер по соблюдению конфиденциальности и защиты персональных данных.

При этом особое внимание следует уделять следующим аспектам:

* Соответствие требованиям законодательства: Необходима регулярная проверка соответствия существующих процессов и технологий актуальным правовым нормам.
* Обучение и просвещение: Важно создавать систему обучения сотрудников по вопросам правовой защиты информации, чтобы повысить уровень осведомлённости и ответственности за соблюдение правовых требований.
* Разработка внутренней документации: Создание и внедрение чётких внутренних политик и регламентов, касающихся обработки и защиты информации в АС.
* Мониторинг и аудит: Регулярный мониторинг и аудит систем безопасности помогут выявить и устранить возможные нарушения правовых норм.

Таким образом, успешная реализация методов правовой защиты информации в автоматизированных системах требует согласованного подхода, включающего юридические, технические и организационные элементы. Это будет способствовать не только защите информации, но и повышению уровня доверия со стороны пользователей и клиентов.