|  |  |
| --- | --- |
| **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 №7

**«ЛИЦЕНЗИРОВАНИЕ ДЕЯТЕЛЬНОСТИ И СЕРТИФИКАЦИЯ СРЕДСТВ В ОБЛАСТИ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ»**

*(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 №7 «ЛИЦЕНЗИРОВАНИЕ ДЕЯТЕЛЬНОСТИ И СЕРТИФИКАЦИЯ СРЕДСТВ В ОБЛАСТИ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ»**

**Исходные данные для проведения работы:**

1. Цель работы. Освоение методов защиты конфиденциальной информации при использовании государственных систем лицензирования и сертификации.

2. Условия работы фирмы аналогичны указанным в ЛР №1.

3. Образцы документов по вопросам лицензирования и сертификации.

4. Лекционный и другой теоретический материал по теме.

**Задание**

1. Обоснуйте необходимость проведения лицензирования выбранного вида деятельности.

2. Укажите порядок и необходимость (обязательная или добровольная) сертификации средств, используемых в выбранном виде деятельности.

3. Укажите перечень сертификационных документов, необходимых для выбранной деятельности фирмы.

4. Составьте для вашей фирмы документы, необходимые для осуществления заданного вида деятельности.

**Ход работы:**

1. Необходимость проведения лицензирования

В России лицензирование в области разработки программного обеспечения не является обязательным для всех видов деятельности, однако в некоторых случаях оно необходимо:

* Регулирование по защите данных: Если "ИнноваТек" будет обрабатывать персональные данные, нужно будет придерживаться Федерального закона № 152-ФЗ "О персональных данных". Некоторые виды обработки могут требовать лицензирования.
* Государственные контракты: Если ваша компания планирует участвовать в государственных закупках, наличие лицензии может быть обязательным.
* Конфиденциальность и безопасность: Лицензирование помогает обеспечить соблюдение правовых норм и стандартов в области безопасности и защиты информации.

2. Порядок и необходимость сертификации

В России сертификация средств разработки программного обеспечения может быть как обязательной, так и добровольной:

* Обязательная сертификация: Для программного обеспечения, которое связано с критически важными или государственными системами, может быть необходима обязательная сертификация. Это может касаться систем, связанных с безопасностью, здравоохранением и т.д.
* Добровольная сертификация: Для других видов ПО сертификация может быть добровольной. Тем не менее, наличие сертификатов может повысить доверие клиентов и продемонстрировать высокие стандарты качества.

3. Перечень сертификационных документов

Для "ИнноваТек" могут потребоваться следующие сертификационные документы:

* Заключения об оценке соответствия.
* Сертификаты соответствия (например, ГОСТ Р).
* Технические условия (ТУ) на разработки.
* Протоколы испытаний.
* Документы по управлению качеством (например, ISO 9001).
* Свидетельства о регистрации ПО (при необходимости).

4. Необходимые документы для осуществления деятельности

Вот перечень документов, необходимых для работы "ИнноваТек":

Учредительные документы:

* Устав фирмы.
* Протокол о создании юридического лица.
* Свидетельство о регистрации юридического лица.
* Лицензия (если требуется в зависимости от видов деятельности).

Договоры с клиентами:

* Договор на разработку программного обеспечения.
* Договор на предоставление ИТ-услуг.
* Договор об обработке персональных данных (если необходимо).

Контракты с поставщиками:

* Соглашения о предоставлении необходимых технологий или оборудования.

Политики и регламенты:

* Политика безопасности информации.
* Регламент обработки персональных данных.

Изучение и внедрение системы менеджмента качества:

* Внутренние регламенты системы качества.
* Проведение внутренних проверок и аудит.

Должностные инструкции для сотрудников, описывающие их обязанности, полномочия и ответственность.

Контрольные вопросы:

1. Нормативно-правовое регулирование

Деятельность в области защиты конфиденциальной информации в России регулируется рядом нормативных документов, включая:

* Федеральный закон № 152-ФЗ "О персональных данных".
* Федеральный закон № 149-ФЗ "Об информации, информационных технологиях и о защите информации".
* Федеральный закон № 382-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части обеспечения безопасности критически важных объектов" (если применимо).

Существующие ГОСТы и СТП в области защиты информации.

2. Виды деятельности, подлежащие лицензированию

Лицензированию подлежат следующие виды деятельности:

* Обработка и хранение персональных данных.
* Разработка и внедрение систем защиты конфиденциальной информации.
* Оказание услуг по обеспечению информационной безопасности.
* Услуги по защите критически важных информационных систем.

3. Порядок лицензирования и срок действия лицензии

* Сбор документов: Подача заявления и необходимых документов в лицензирующий орган.
* Рассмотрение заявления: Проверка предоставленных документов и, возможно, проведение проверки.
* Выдача лицензии: При положительном решении выдаётся лицензия.
* Срок действия: Лицензия в России, как правило, выдается на неопределенный срок, но должна регулярно подтверждаться.

4. Организационная структура системы сертификации

Организационная структура включает:

* Федеральные органы власти (например, ФСБ, Роскомнадзор).
* Организации, уполномоченные на проведение сертификации.
* Аккредитованные испытательные лаборатории.
* Подразделения по сертификации в различных министерствах и ведомствах.

5. Организации, имеющие системы сертификации в РФ

* ФСБ России: Занимается сертификацией средств защиты информации.
* Федеральный центр технической и экспортной безопасности.
* НТК принадлежности (Некоторые негосударственные организации).
* Росстандарт: Важные аккредитационные и сертификационные центры.

6. Порядок и требования при сертификации

* Заявка на сертификацию: Подготовка соответствующих документов и их подача.
* Технические испытания: Проведение испытаний сертификованных средств защиты информации.
* Аудит: Проверка соответствия заявленным требованиям.
* Выдача сертификата: После успешного прохождения всех процедур.

7. Добровольная сертификация

Сертификация носит добровольный характер в случаях:

* Когда речь идет о программном обеспечении и системах, не относящихся к критически важным.
* Для продуктов, которые не попадают под обязательное лицензирование или сертификацию, но могут повысить доверие клиентов.

8. Установление форм сертификата и знака соответствия

* Формы сертификата и знака соответствия устанавливаются:
* Федеральными органами стандартизации, такими как Росстандарт.
* Уполномоченными органами по сертификации.

9. Российские и международные стандарты безопасности

Российские стандарты:

* ГОСТ Р 50922-96 (Защита информации. Общие требования).
* ГОСТ Р 51275-99 (Защита информации в автоматизированных системах).

Международные стандарты:

* ISO 27001 (Системы менеджмента безопасности информации).
* ISO 27002 (Руководство по управлению безопасностью информации, содержащей контрольные меры).
* NIST SP 800-53 (Контроль безопасности и конфиденциальности).

Вывод: Цель данной работы – освоение методов защиты конфиденциальной информации через использование государственных систем лицензирования и сертификации – является важной и актуальной. Эффективная защита конфиденциальных данных требует глубокого понимания нормативно-правовых актов, механизмов лицензирования и сертификации, а также применения международных стандартов.

Освоение этих методов позволяет не только обеспечить безопасность информации, но и повысить доверие пользователей к информационным системам. Кроме того, применение государственных стандартов и аккредитаций помогает минимизировать риски утечек данных и нарушений законодательства, что является критически важным в условиях современного цифрового мира.