**Лабораторная работа №9**

**Тема**: «Стандарты информационной безопасности»

**Цель**: «Изучить стандарты информационной безопасности»

**Задача №1**

*Цель*: обеспечение информационной безопасности при передаче

ответственности за обработку информации другой организации. Изучить

разделы ГОСТ Р ИСО/МЭК 27002-2012.

*Ответ*:

1. **Идентификация информации:**
   * Определите какие конкретные данные и информацию необходимо передавать сторонним организациям;
   * Оцените степень конфиденциальности и важности этих данных;
   * Определите, какие сторонние организации будут вовлечены в обработку информации.
2. **Риски и оценка рисков:**
   * Проведите анализ рисков, связанных с передачей информации сторонним организациям;
   * Оцените уровень угроз и уязвимостей при обработке данных сторонними организациями;
   * Оцените потенциальные последствия инцидентов в области информационной безопасности.
3. **Разработка политики и процедур:**
   * Разработайте политику и процедуры, которые определяют условия передачи данных сторонним организациям;
   * Включите в политику меры по обеспечению конфиденциальности, целостности и доступности данных.
4. **Соглашения и контракты:**
   * Разработайте соглашения и контракты, которые определяют права и обязанности в области информационной безопасности для сторонних организаций;
   * Включите в контракты меры по мониторингу и аудиту информационной безопасности сторонних организаций.
5. **Обучение и осведомление:**
   * Обучите сотрудников вашей организации о правилах и процедурах взаимодействия с сторонними организациями в рамках информационной безопасности;
   * Обеспечьте осведомленность сотрудников о рисках и мероприятиях в области информационной безопасности.
6. **Инциденты информационной безопасности:**
   * Разработайте процедуры управления инцидентами в области информационной безопасности для реагирования на возможные инциденты с данными, передаваемыми сторонними организациями.
7. **Оценка эффективности:**
   * Периодически оценивайте эффективность мероприятий и корректируйте их в соответствии с изменениями рисков и требований.
8. **Документация и обучение:**

* Внимательно документируйте все мероприятия и соглашения в области информационной безопасности.

**Задача №2**

*Вопрос*: имеет ли место в данной ситуации нарушение авторского права гражданина Смирнова?

*Ответ*: В данной ситуации имеет место нарушение авторского права гражданина Смирнова согласно статье 1229 части 4 Гражданского кодекса Российской Федерации.

Статья 1229 ГК РФ устанавливает, что автор имеет право на охрану своего произведения. Авторские права включают в себя право на создание производных произведений. В данной ситуации гражданин Смирнов передал компании "MosTechnology" имущественные права на распространение программного продукта "Albert 3D", **!но!** это не означает, что компания имеет право модифицировать программу без согласия автора.

Поэтому, если "MosTechnology" внесла предварительные модификации в программу "Albert 3D" без согласия автора => нарушение авторские права гражданина Смирнова.

**Задача №3**

*Вопросы*:

1. Какая статья УК РФ была нарушена?
2. Что послужило предметом преступления?
3. Какие неправомерные информационные действия были совершены А.Н. Ивановым?

*Ответ*:

1. А.Н. Иванов нарушил статью 273 Уголовного кодекса РФ, которая относится к компьютерной мошенничеству. Конкретно, это может быть часть 3 данной статьи.
2. Предметом преступления была компьютерная банковская система и внедренный вирус, который уничтожил исполняемые файлы (.exe), принадлежащие банку.
3. А.Н. Иванов совершил следующие неправомерные (информационные) действия:
4. Внедрение вредоносного вируса в компьютерную систему банка.
5. Уничтожение исполняемых файлов банковских программных приложений, что привело к материальному ущербу для банка.
6. Совершение данных действий без согласия и разрешения компетентных органов и вопреки интересам банка, что является неправомерным доступом к информационным ресурсам.

**Задача №4**

*Цель*: обеспечение информационной безопасности при хранении, обработке, передаче и уничтожении информации

*Ответ*: основные требования, которые могут быть полезны:

1. **Классификация информации:**
   * Определение категорий информации по степени конфиденциальности (например, общедоступная, внутренняя, конфиденциальная, секретная);
   * Установление правил для маркировки и классификации информации.
2. **Доступ к информации:**
   * Управление доступом к информации на принципе "необходимости знания";
   * Установление процедур аутентификации и авторизации для доступа к информации;
   * Ограничение физического доступа к информационным ресурсам.
3. **Хранение информации:**
   * Определение мест хранения информации, включая серверы, файловые хранилища, бумажные документы и т.д.;
   * Установление мер безопасности для защиты хранимой информации, включая шифрование данных, резервное копирование и физическую защиту серверов.
4. **Обработка информации:**
   * Установление правил и процедур обработки информации, включая соблюдение принципов целостности и конфиденциальности;
   * Обучение сотрудников по правилам обработки информации.
5. **Передача информации:**
   * Определение процедур для безопасной передачи информации, включая защищенную передачу по сети и использование шифрования;
   * Установление правил для обмена информацией с внешними сторонами (партнерами, клиентами) и контроль передачи конфиденциальных данных.
6. **Уничтожение информации:**
   * Определение процедур и сроков уничтожения информации, включая физическое уничтожение бумажных документов и безвозвратное удаление электронных данных;
   * Поддержание журналов уничтожения для отслеживания процесса.
7. **Мониторинг и аудит:**
   * Установление системы мониторинга и аудита для отслеживания действий пользователей и обнаружения инцидентов в области информационной безопасности;
   * Регулярная проверка соответствия политик и требований.
8. **Обучение и осведомленность:**
   * Обучение сотрудников в области информационной безопасности и их осведомленность о правилах и процедурах;
   * Регулярное информирование сотрудников о новых угрозах и мероприятиях по обеспечению информационной безопасности.
9. **Инциденты информационной безопасности:**
   * Разработка процедур управления инцидентами и реагирования на нарушения информационной безопасности.
10. **Соблюдение законодательства:**
    * Обязательное соблюдение всех применимых законов и нормативных актов, связанных с информационной безопасностью.

**Задача №5**

*Цель*: уведомление новых сотрудников о строгом выполнении требований по обеспечению информационной безопасности и ответственности за их нарушение.

*Ответ*: вот несколько ключевых требований для специалистов по подбору кадров:

1. **Понимание информационной безопасности:** Специалисты по подбору кадров должны иметь глубокое понимание информационной безопасности и знать ее важность для организации.
2. **Знание политики информационной безопасности:** они должны быть хорошо знакомы с существующей политикой информационной безопасности в организации, включая стандарты и процедуры.
3. **Согласование требований:** Специалисты по подбору кадров должны работать в тесном сотрудничестве с отделом информационной безопасности, чтобы гарантировать, что требования по информационной безопасности согласованы с политикой организации.
4. **Интеграция в процесс подбора:** они должны внедрить требования по информационной безопасности в процесс подбора кадров, включая вопросы об информационной безопасности в собеседованиях и анкетах для кандидатов.
5. **Информирование и обучение кандидатов:** Специалисты по подбору кадров должны уведомлять кандидатов о важности информационной безопасности и обязанностях в этой области. Это может включать в себя проведение информационных сессий или предоставление руководств по информационной безопасности.
6. **Внесение в трудовой договор:** они должны внести соответствующие пункты о информационной безопасности в трудовой договор новых сотрудников, включая ответственность за соблюдение политики информационной безопасности.
7. **Мониторинг и соблюдение:** Специалисты по подбору кадров должны следить за соблюдением требований информационной безопасности и обязательств новых сотрудников в этой области.
8. **Обратная связь и улучшение:** они должны поддерживать обратную связь с отделом информационной безопасности и участвовать в улучшении процессов подбора кадров с учетом информационной безопасности.

**Контрольные вопросы:**

1. Основополагающие документы по информационной безопасности могут включать:
   * Концепция информационной безопасности организации;
   * Политика информационной безопасности;
   * Стандарты и регламенты организации (например, ГОСТы);
   * Положения и инструкции по обеспечению информационной безопасности;
   * Оранжевая книга;
   * Соглашения и контракты с партнерами и сторонними организациями;
   * Законы и нормативные акты о информационной безопасности.
2. Государственная тайна — это информация, составляющая государственную, военную или иную охраняемую законом тайну, предназначенная для обеспечения интересов Российской Федерации и подвергающаяся специальной защите. Раскрытие государственной тайны без разрешения компетентных органов является уголовным преступлением.
3. Основные задачи информационной безопасности в соответствии с концепцией национальной безопасности РФ включают в себя:
4. Защиту информации от утечки и несанкционированного доступа;
5. Обеспечение кибербезопасности и защиты критической информационной инфраструктуры;
6. Предотвращение кибератак и борьба с киберпреступностью;
7. Защиту государственных информационных ресурсов и интересов РФ в киберпространстве;
8. Обеспечение информационной безопасности граждан и бизнеса.
9. Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" устанавливает правила и требования в области информационной безопасности, регулирует отношения, связанные с обработкой и защитой информации. Закон определяет права и обязанности субъектов информационных отношений, а также устанавливает меры ответственности за нарушение требований закона
10. В Уголовном кодексе РФ предусмотрена ответственность за создание, использование и распространение вредоносных компьютерных программ в соответствии с статьей 273.1 УК РФ. Наказание может включать в себя штраф и/или лишение свободы в зависимости от характера преступления и его последствий.
11. Функциональные требования стандарта ГОСТ Р ИСО/МЭК 15408-1-2012 (ISO/IEC 15408-1:2009) касаются оценки безопасности информационных систем. Некоторые из них включают:
    * Аутентификация;
    * Авторизация;
    * Контроль доступа;
    * Аудит и мониторинг безопасности;
    * Защита от вредоносных программ;
    * Защита от несанкционированного доступа.
12. Профиль защиты, согласно стандарту ГОСТ Р ИСО/МЭК 15408-1-2012, описывает конкретные требования и функции, которые должны быть реализованы в информационной системе для обеспечения её безопасности. Он является основой для оценки соответствия информационной системы установленным стандартам и требованиям безопасности.
13. Доктрина информационной безопасности РФ — это официальный документ, который устанавливает основные положения и принципы обеспечения информационной безопасности Российской Федерации. В ней определяются угрозы и вызовы в области информационной безопасности, принципы государственной политики в этой области, а также меры по обеспечению информационной безопасности страны. Доктрина также описывает роли и обязанности государственных и общественных структур в обеспечении информационной безопасности России.