МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Казанский национальный исследовательский технический университет

им. А.Н. Туполева – КАИ»

Институт компьютерных технологий и защиты информации

Отделение СПО ИКТЗИ (Колледж информационных технологий)

ЛАБОРАТОРНАЯ РАБОТА №3

по дисциплине

Основы алгоритмизации и программирования

Тема: «Обоснование применения норм уголовного права в конкретных ситуациях и нахождение применимых правовых норм в заданных условиях.»

Работу выполнил

Студент гр.4233

Логинов Д.А.

Принял

Преподаватель Кожевников. К.Д.

Казань 2024

**Часть №1**

**Цель**

Обосновать применение норм правового наказания при использовании ВПО

а) **Вопрос:** Вы пишите на заказ на программы, которые заражает компьютер и подгружают вредоносные программы. При этом сами данным программным обеспечение не пользуетесь.

**Ответ:** в данной ситуации лицо пишет программное обеспечение, которое заражает компьютеры и устанавливает вредоносное ПО, но при этом сам не использует данное программное обеспечение. Согласно статьям 273 - 276 УК РФ, за создание, использование и распространение вредоносных программ предусмотрена уголовная ответственность. В данной ситуации мы являемся разработчиком вредносных программ, что также является не правильным.

b) **Вопрос:** Системный администратор некоторой известной компании без ведома устанавливал по сети всем программу для удаленного

администрирования RAdmin.

# Ответ: Системный администратор устанавливал программу для удаленного администрирования без ведома пользователей. Действия системного администратора могут быть квалифицированы как нарушение конфиденциальности (статья 138 УК РФ), что также может нести уголовную ответственность.

# Также такое нарушение может быть обработано Федеральным законом "О персональных данных" от 27.07.2006 N 152-ФЗ в случае если данные будут распространяться третьим лицам или 276 УК РФ «Шпионаж»

c) **Вопрос:** Вы случайно распространили по сети вирус, который шифрует данные на ПК пользователей

**Ответ:** Распространение вируса, который шифрует данные на ПК пользователей, влечет за собой уголовную ответственность согласно статьям 273 - 276 УК РФ. Но с точки зрения человечности, можно, я считаю, понять и простить, так как действие распространения вируса было не преднамеренным и не специальным.

d) **Вопрос:** Вы не распространяли вирус, но выложили его на GitHub.

**Ответ:** Выкладывание вируса на GitHub тоже может быть расценено как распространение вредоносного программного обеспечения и подпадает под статьи 273 - 276 УК РФ.

e ) **Вопрос:** Вам 17 лет, ради интереса распространили вредоносное программное обеспечение.

**Ответ:** Распространение вредоносного программного обеспечения вне зависимости от возраста лица также соответствует статьям УК РФ о незаконном использовании ПО. Данное действие влечет за собой 273 ст. УК РФ «О распространении ВПО»

f) **Вопрос:** Вы разработали код вредоносной программы, но еще не воспользовались им.

**Ответ:** Разработка кода вредоносной программы без фактического использования также несет уголовную ответственность согласно статьям 273 - 276 УК РФ.

g) **Вопрос:** Вы гражданин РФ и используете вредоносное программное обеспечение исключительно за пределами Российской Федерации

**Ответ:** Использование вредоносного программного обеспечения за пределами России также может быть рассмотрено с точки зрения международного сотрудничества в борьбе с киберпреступностью.

**Контрольные вопросы**

1. **Использование** **нелицензионного** **программного** **обеспечения** является нарушением авторских и смежных прав и влечет за собой административную (ст. 7.12. КоАП РФ), уголовную (ст. 146 УК РФ) и гражданско-правовую **ответственность**.
2. 1. Выберите подходящую лицензию: Существует множество различных типов лицензий (например, проприетарная, открытая и др.), каждая из которых имеет свои особенности и требования. Уделите внимание выбору лицензии, которая соответствует вашим целям и философии разработки.

2. Определите права и обязанности: Лицензия программного обеспечения должна четко определять права и обязанности как правообладателя, так и пользователей. Это поможет избежать недопониманий и споров.

3. Укажите ограничения использования: В лицензии должны прописываться ограничения по использованию программы (например, запрет коммерческого использования, копирование, модификация и т.д.), если таковые имеются.

4. Установите срок действия: Некоторые лицензии имеют ограниченный срок действия. Укажите в лицензии срок ее действия и условия его продления или прекращения.

5. Защитите свои авторские права: Убедитесь, что в лицензии отражены все ваши авторские права на программное обеспечение и они защищены соответствующим образом.

6. Контроль за соблюдением лицензии: Предусмотрите механизмы контроля за соблюдением условий лицензионного соглашения, например, путем ведения учета лицензий и регулярной проверки использования программы.

7. Получите консультацию юриста: Лицензирование программного обеспечения может быть сложным процессом. Важно проконсультироваться с опытным юристом или специалистом по защите интеллектуальной собственности, чтобы убедиться в соблюдении всех необходимых норм и правил.

**Часть №2**

**Цель**

Ознакомиться с правовой сферой в области информационной безопасности

**Охарактеризация документов с точки зрения информационной безопасности:**

1. **Конституция Российской Федерации:** Определяет основные принципы государственного устройства и права граждан, включая защиту информации и конфиденциальности.

2. **Федеральный закон «Об информации, информационных технологиях и о защите информации»:** Содержит нормы по охране информации, обеспечение безопасности информационных систем.

3. **Федеральный закон «О коммерческой тайне»:** Регулирует вопросы коммерческой тайны и защиты конфиденциальной информации компаний.

4. **Федеральный закон «О персональных данных»:** Устанавливает правила сбора, хранения и обработки персональных данных граждан.

5. **«Уголовный кодекс Российской Федерации»:** Содержит нормы, касающиеся противоправных действий в области информационной безопасности и их наказания.

6. **Указ Президента РФ о мерах по обеспечению информационной безопасности:** Определяет меры по защите информационной безопасности при использовании информационно-телекоммуникационных сетей.

**Основные положения относящиеся к информационной безопасности:**

1. **Охрана государственной тайны и коммерческой тайны:** Законы об обеспечении конфиденциальности информации.

2. **Обработка персональных данных:** Нормы по обработке и защите персональных данных граждан.

3. **Нормы противодействия преступлениям в сфере информационных технологий:** Установление ответственности за противоправные действия и атаки на информационные системы.

4. **Требования к информационной безопасности:** Установление стандартов и мер по обеспечению безопасности информации и информационных систем.

**Контрольные вопросы**

1. **Законодательные меры в области информационной безопасности необходимы для:**

- **Защиты конфиденциальной информации:** Обеспечение безопасности и неразглашения чувствительных данных.

- **Предотвращения кибератак и нарушений безопасности:** Установление правил и ответственности для защиты информации от вредоносных действий. - **Регулирования сбора и обработки персональных данных:** Ограничение и контроль за использованием персональной информации граждан.

- **Обеспечения надежности информационных систем:** Гарантия стабильности и защиты информационных технологий.

2. **Документы, регулирующие информационную безопасность в Российской Федерации:**

В Российской Федерации информационная безопасность регулируется следующими основными документами:

- **Конституция Российской Федерации:** Включает положения о защите информации и конфиденциальности.

- **Федеральные законы:** Например, Федеральный закон «О безопасности», «Об информации, информационных технологиях и о защите информации», «О персональных данных» и другие, устанавливающие нормы и правила в области информационной безопасности.

- **Постановления и указы Президента РФ:** К примеру, указы, определяющие меры по обеспечению информационной безопасности в стране.

**Основополагающие документы в области информационной безопасности:**

3. Некоторые из основополагающих документов в области информационной безопасности в Российской Федерации включают:

- **Конституция Российской Федерации:** Как основной закон страны, определяющий общие принципы защиты информации и прав граждан.

- **Федеральный закон «О персональных данных»:** Регулирует сбор, хранение и обработку информации о гражданах.

- **Федеральный закон «Об электронной подписи»:** Устанавливает правила использования электронных подписей в целях обеспечения доверия к электронным документам.