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 в ИКТЗИ (Колледж информационных технологий)

ЛАБОРАТОРНАЯ РАБОТА №3

по дисциплине

Информационная безопасность

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

Работу выполнил

Студент гр.4237

Каримов М.И

Принял

Преподаватель Кожевников К.Д.

Казань 2024

**1 часть**

a) Статья 273 УК РФ предусматривает уголовную ответственность за создание вредоносных компьютерных программ, независимо от того, использовали вы их или нет. Санкция может включать штрафы, принудительные работы до 4 лет или лишение свободы на тот же срок.

Я считаю, что создание таких программ может быть законно в зависимости от контекста. Если человек их делает для тестирования ПО, то это окей. Если для злого умысла, то не окей.

Если программа создается для законных целей тестирования безопасности и улучшения антивирусных программ, это способствует повышению стойкости к кибератакам. Этичный хакинг важен для выявления и исправления уязвимостей систем.

Создание и распространение вредоносного ПО с целью нанесения ущерба или получения незаконной выгоды подрывает информационную безопасность и влечет за собой серьезные нарушения закона.

b) Если системный администратор устанавливал программы без ведома пользователей, это может рассматриваться как неправомерное воздействие на компьютерную информацию (статья 272 УК РФ) или как распространение вредоносных программ, если эта программа нанесла вред (статья 273 УК РФ).

Если он не владелец компании, то это безусловно плохо. Данный сотрудник подлежит увольнению.

Правомерное использование таких программ администраторами ИТ-систем может быть эффективным инструментом для обеспечения поддержки и обслуживания компьютеров на расстоянии.

Если администрирование осуществляется без согласия пользователей, это нарушает приватность и может быть использовано для незаконного доступа к конфиденциальным данным.

c) Распространение вирусов, даже неумышленное, может подпадать под статью 273 УК РФ, в зависимости от ущерба, который причинен вирусом. Ответственность может быть разной, включая лишение свободы до 4 лет.

Все равно это распространение и уголовно наказуемо.

Может служить предупреждением для улучшения мер безопасности и разработки стратегий защиты от аналогичных инцидентов в будущем.

Ошибка может привести к массовым нарушениям работы компьютерных систем, потере данных и доверия пользователей.

d) Размещение вирусов на платформе разработчиков вроде GitHub также может быть классифицировано по статье 273 УК РФ как распространение вредоносных программ.

Публикация с исследовательской целью может содействовать развитию науки о кибербезопасности и дать сообществу необходимые знания для защиты от подобных угроз.

Доступ к вирусу может быть использован недобросовестными людьми для создания новых вариантов вредоносного ПО и распространения его в интернете.

e) Даже если вам нет 18 лет, распространение вредоносного ПО может повлечь за собой уголовную ответственность. Обычно возраст влияет на выбор вида и размера наказания.

Подростки могут совершать ошибки из-за неопытности, но это может стать мощным уроком о законе и этике, который изменит их жизнь в лучшую сторону.

Даже юношеские проступки могут привести к серьезным юридическим последствиям и нанести ущерб репутации на долгие годы.

f) Разработка вредоносного кода также может рассматриваться по статье 273 УК РФ, однако применение санкций зависит от действий после создания кода.

Работа над кодом может быть частью научного проекта для изучения природы вредоносного ПО и укрепления методов его обнаружения.

Сама разработка может быть истолкована как подготовка к киберпреступлению и использована для создания инструментов для атак.

g) Использование вредоносного ПО за пределами РФ может подпасть под юрисдикцию других стран, однако российское законодательство также может применяться в случаях, указанных в Уголовном кодексе РФ.

В случае если человек занимается тестированием международных сетевых структур на устойчивость к атакам, то это может быть связано с профессиональной деятельностью.

Преднамеренное использование вредоносного ПО за пределами страны может наносить ущерб интересам других государств и приводить к международным конфликтам.

**Контрольные вопросы 1 части**

1. Виды ответственности за использование нелицензионного программного обеспечения включают:

- Административная ответственность: Применение штрафов к физическим и юридическим лицам за нарушение авторских прав (ст. 7.12 КоАП РФ).

- Гражданско-правовая ответственность: Взыскание убытков в пользу правообладателя, которые вызваны использованием нелицензионного ПО.

- Уголовная ответственность: Может включать штрафы, принудительные работы или лишение свободы, в зависимости от тяжести преступления (статьи 146, 272, 273 УК РФ).

2. Чтобы правильно лицензировать программное обеспечение:

- Приобретите ПО у официальных дистрибьюторов или напрямую у разработчиков.

- Обеспечьте соответствие приобретенных лицензий количеству используемых копий программы.

- Постоянно отслеживайте и контролируйте использование лицензионного ПО в организации, чтобы избежать использования программного обеспечения сверх числа приобретенных лицензий.

- Регулярно проверяйте условия лицензионных соглашений, поскольку они могут изменяться.

- Используйте системы управления активами для мониторинга и управления лицензиями программного обеспечения.

- Обучайте сотрудников принципам лицензирования и аудита программного обеспечения для соблюдения законодательства.

Виды ответственности за использование нелицензионного программного обеспечения включают в себя:

1. Гражданскую ответственность: это означает, что пользователь может быть привлечен к ответственности за нарушение авторских прав, что может привести к уплате штрафов или компенсации ущерба правообладателю.

2. Уголовную ответственность: в некоторых странах использование нелицензионного программного обеспечения может быть преступлением, что может привести к аресту, штрафам или другим юридическим мерам.

3. Этическую ответственность: использование нелицензионного программного обеспечения противоречит этическим принципам и может нанести ущерб репутации пользователя. Это как минимум не красиво и подвергается осуждению.

Как правильно лицензировать программное обеспечение:

1. Покупка лицензии у производителя: Для правильной лицензирования программного обеспечения вам следует обратиться к производителю ПО или его официальным партнерам для покупки лицензии на использование программы.

2. Ознакомление с лицензионным соглашением: После приобретения лицензии важно внимательно прочитать лицензионное соглашение, чтобы понять условия использования программного обеспечения.

3. Соблюдение условий лицензионного соглашения: Необходимо строго соблюдать условия лицензионного соглашения, такие как количество лицензируемых копий, период использования, область применения и другие ограничения.

4. Регулярное обновление и поддержка лицензии: Следите за сроком действия лицензии и обновляйте ее вовремя, чтобы избежать нарушений.

Для конкретной информации о лицензировании определенного программного обеспечения важно обращаться к производителю или официальным источникам информации, таким как официальные сайты производителей.

**2 часть**

1. Конституция Российской Федерации: Она неоднократно подтверждает право граждан на конфиденциальность и защиту их личных данных.

2. Федеральный закон от 28.12.2010 № 390-ΦЗ «О безопасности»: Основные принципы и требования к обеспечению информационной безопасности.

3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: Устанавливает правила по обработке и защите информации.

4. Закон РФ «О государственной тайне» от 21.07.1993: Регулирует порядок обращения с информацией, составляющей государственную тайну.

5. Федеральный закон «О коммерческой тайне» от 29.07.2004: Защищает информацию, считающуюся коммерческой тайной.

6. Федеральный закон «О персональных данных» от 27.07.2006: Устанавливает правила обработки и защиты персональных данных.

7. Федеральный закон «Об электронной подписи» от 06.04.2011: Регулирует использование электронной подписи для обеспечения целостности информации.

8. Уголовный кодекс Российской Федерации от 13.06.1996: Включает преступления в сфере информационной безопасности.

9. Трудовой кодекс Российской Федерации от 30.12.2001: Возможно, регулирует вопросы охраны информации на рабочем месте.

10. Кодекс об административных правонарушениях: Содержит административные наказания за нарушения законодательства в области информационной безопасности.

11. Указ Президента РФ от 17.03.2008 № 351: Меры по обеспечению информационной безопасности при использовании информационно-телекоммуникационных сетей.

Эти документы устанавливают правила и нормы в области информационной безопасности, защиты конфиденциальной информации и персональных данных, а также определяют ответственность за нарушения в этой сфере.

**Контрольные вопросы 2 части**

1. Законодательные меры в области информационной безопасности необходимы для обеспечения защиты информации от несанкционированного доступа, использования, модификации или уничтожения. Это важно для обеспечения конфиденциальности, целостности и доступности информации, защиты от киберугроз, предотвращения кибератак и обеспечения безопасности информационных ресурсов.

2. Информационная безопасность в Российской Федерации регулируется рядом законодательных актов, включая Федеральный закон "Об информации, информационных технологиях и о защите информации", Федеральный закон "О персональных данных", а также Постановления Правительства РФ и другие нормативные документы.

3. Основополагающие документы в области информационной безопасности, с которыми я знакома, включают в себя:

- Федеральный закон "Об информации, информационных технологиях и о защите информации"

- Федеральный закон "О персональных данных"

- Концепция обеспечения информационной безопасности в Российской Федерации

- Доктрина информационной безопасности Российской Федерации

- Стратегия информационной безопасности Российской Федерации