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

Информационная безопасность

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

Работу выполнил

Студент гр.4233

Давлетшин К. У.

Принял

Преподаватель Кожевников К. Д.

Казань 2024

**Задание на лабораторную работу**

**Часть №1**

**Цель работы**

Обосновать применение норм правового наказания при использовании ВПО

**Методические указания**

1. Проанализируйте приведенные ниже ситуации.

2. Ссылаясь на статьи «Уголовного кодекса Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 02.08.2019), какую ответственность несут люди в данных ситуациях.

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

b) Системный администратор некоторой известной компании без ведома устанавливал по сети всем программу для удаленного администрирования RAdmin.

c) Вы случайно распространили по сети вирус, который шифрует данные на ПК пользователя.

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

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

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

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

**Контрольные вопросы**

1. Перечислите виды ответственности за использование не лицензионного программного обеспечения?

2. Как правильно лицензировать программное обеспечение?

**Часть №2**

**Цель работы** -Ознакомиться с правовой сферой в области информационной безопасности

**Методические указания**

1. Ознакомьтесь со следующими документами:

Конституция Российской Федерации http://www.constitution.ru/

Федеральный закон от 28.12.2010 № 390-ΦЗ «О безопасности» http://www.consultant.ru/document/cons\_doc\_LAW\_108546/

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» http://www.consultant.ru/document/cons\_doc\_LAW\_61798/

Закон РФ «О государственной тайне» от 21.07.1993 http://www.consultant.ru/document/cons\_doc\_LAW\_2481/

Федеральный закон «О коммерческой тайне» от 29.07.2004 http://www.consultant.ru/document/cons\_doc\_LAW\_48699/

Федеральный закон «О персональных данных» от 27.07.2006 http://www.consultant.ru/document/cons\_doc\_LAW\_61801/

Федеральный закон «Об электронной подписи» от 06.04.2011 http://www.consultant.ru/document/cons\_doc\_LAW\_112701/

«Уголовный кодекс Российской Федерации» от 13.06.1996 http://www.consultant.ru/document/cons\_doc\_LAW\_10699/

«Трудовой кодекс Российской Федерации» от 30.12.2001 http://www.consultant.ru/document/cons\_doc\_LAW\_34683/

Кодекс РФ об административных правонарушениях http://www.consultant.ru/document/cons\_doc\_LAW\_34661/

Указ Президента РФ от 17.03.2008 № 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» http://www.consultant.ru/document/cons\_doc\_LAW\_75586/

2. Охарактеризуйте данные документы с точки зрения информационной безопасности

3. Выделите основные положения, которые относятся к информационной безопасности

**Контрольные вопросы**

1. Для чего нужны законодательные меры в области информационной безопасности?

2. Какими документами регулируется информационная безопасность в Российской Федерации?

3. Какие основополагающие документы в области информационной безопасности вам известны?

**Ход выполнения работы**

**Часть №1**

а) Не ссылаясь на законы и говоря с точки зрения человечности и природной интуиции, можно сказать, что в данной ситуации мы поступаем «неправильно», так как мы пишем вредоносные программы под видом обычных, тем самым просто заражаем систему других пользователей. Можно предположить, что в данной ситуации нами движет «неправильный» вид заработка.

Ссылаясь на законы, можно сказать, что данная ситуация подходит под статью №273.1 «Создание, использование и распространение вредоносных компьютерных программ» и можно предположить статью №274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»

b) Не ссылаясь на законы и говоря с точки зрения человечности и природной интуиции, можно сказать, что в данной ситуации человек поступает «неправильно», так как можно предположить, что данные некой известной компании явно не должны попасть в общий доступ или быть использованы в своих целях.

Ссылаясь на законы, можно сказать, что данная ситуация подходит под статью №138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» и под федеральный закон «О безопасности»

с) Не ссылаясь на законы и говоря с точки зрения человечности и природной интуиции, можно сказать, что в данной ситуации мы неумышленно поступаем неправильно, так как мы случайно распространили вирус, который наносит ущерб другим пользователям.

Ссылаясь на законы, можно сказать, что данная ситуация подходит под статью №273 «Создание, использование и распространение вредоносных компьютерных программ».

d) Не ссылаясь на законы и говоря с точки зрения человечности и природной интуиции, можно сказать, что в данной ситуации мы все равно поступаем неправильно, ведь мы умышленно, отводя от себя ответственность, выложили готовый вирус на всеобщее обозрение заведомо зная, что данные действия могут повлечь за собой последствия для других пользователей.

Ссылаясь на законы, можно сказать, что данная ситуация подходит под статью №273 «Создание, использование и распространение вредоносных компьютерных программ».

e) Не ссылаясь на законы и говоря с точки зрения человечности и природной интуиции, можно сказать, что в данной ситуации мы поступаем неправильно, ведь мы умышленно распространяем вредоносное ПО, тем самым наносим умышленный ущерб другим пользователям.

Ссылаясь на законы, можно сказать, что данная ситуация подходит под статью №273 «Создание, использование и распространение вредоносных компьютерных программ».

f) Не ссылаясь на законы и говоря с точки зрения человечности и природной интуиции, можно сказать, что в данной ситуации мы стоим у двух дорог, но вредоносное ПО у нас готово, но мы им никак не воспользовались, мы можем его полностью удалить, тем самым не будем нести никакой ответственности.

Ссылаясь на законы, можно сказать, что данная ситуация подходит под статью №273 «Создание, использование и распространение вредоносных компьютерных программ».

g) Не ссылаясь на законы и говоря с точки зрения человечности и природной интуиции, можно сказать, что в данной ситуации мы поступаем «неправильно», ведь мы все равно используем его, и неважно где.

Использование вредоносного программного обеспечения за пределами Российской Федерации не освобождает гражданина РФ от ответственности. Если такое деяние приведет к угрозе или ущербу для информационной безопасности России, лицо может быть привлечено к ответственности в соответствии с российским законодательством.

**Ответы на контрольные вопросы**

1. Виды ответственности за использование нелицензионного программного обеспечения могут включать:

- Гражданско-правовую ответственность, когда лицо, использующее нелицензионное ПО, может быть привлечено к ответственности по требованию правообладателя на возмещение ущерба.

- Административную ответственность, предусмотренную законодательством страны за нарушение авторских прав, в частности за использование нелицензионного программного обеспечения.

- Уголовную ответственность в случае особо тяжких нарушений авторских прав, которая может привести к уголовному преследованию и наказанию в виде штрафа или даже лишения свободы.

2. Правильная лицензировка программного обеспечения включает в себя следующие шаги:

- Приобретение лицензии у официального правообладателя или авторизованного дистрибьютора программного продукта.

- Внимательное ознакомление с условиями лицензионного соглашения, в котором указаны права и обязанности пользователя.

- Соблюдение условий лицензионного соглашения, включая запрет на передачу или распространение лицензионного ПО без согласия правообладателя.

**Часть №2**

Федеральный закон "О безопасности" устанавливает основные принципы и меры по обеспечению информационной безопасности в России, включая защиту государственной информации, организацию системы обеспечения безопасности, регулирование деятельности в этой области, борьбу с киберугрозами и киберпреступлениями, а также международное сотрудничество.

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» определяет правовые основы обращения с информацией, регулирует использование информационных технологий и устанавливает меры по защите информации от неправомерного доступа, модификации и распространения.

Закон РФ «О государственной тайне» от 21.07.1993 устанавливает порядок обращения с государственной тайной, определяет органы, ответственные за ее защиту, и предусматривает меры по предотвращению утечки государственной тайны.

Федеральный закон «О коммерческой тайне» от 29.07.2004 регулирует отношения, связанные с созданием, использованием и защитой коммерческой тайны, а также устанавливает ответственность за ее неправомерное раскрытие или использование.

Федеральный закон «О персональных данных» от 27.07.2006 определяет правовые основы сбора, обработки и защиты персональных данных граждан, устанавливает требования к их обработке и хранению, а также определяет права субъектов данных.

Федеральный закон «Об электронной подписи» от 06.04.2011 устанавливает правила использования электронной подписи для обеспечения подлинности и целостности электронных документов, а также нормы, регулирующие деятельность сертификационных центров.

«Уголовный кодекс Российской Федерации» от 13.06.1996 содержит статьи, касающиеся ответственности за нарушения в сфере информационной безопасности, включая создание и распространение вредоносных программ, незаконный доступ к информации и другие действия.

«Трудовой кодекс Российской Федерации» от 30.12.2001 устанавливает правила использования информации в рабочих отношениях, включая соблюдение конфиденциальности и защиту информации организации.

Кодекс РФ об административных правонарушениях определяет административные наказания за нарушения законодательства в области информационной безопасности, такие как незаконный доступ к информации или нарушение правил обращения с государственной и коммерческой тайной.

Указ Президента РФ от 17.03.2008 № 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» определяет меры по обеспечению безопасности информации в информационно-телекоммуникационных сетях при международном информационном обмене.

Основные положения, относящиеся к информационной безопасности в указанных законах:

1. Конституция Российской Федерации:

- Гарантирует право на конфиденциальность переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений.

2. Федеральный закон "О безопасности":

- Определяет основные принципы обеспечения безопасности, включая информационную безопасность, и устанавливает обязанности государственных органов, организаций и граждан в этой области.

3. Федеральный закон "Об информации, информационных технологиях и о защите информации":

- Регулирует использование информационных технологий и устанавливает меры по защите информации от неправомерного доступа, модификации и распространения.

4. Закон РФ "О государственной тайне":

- Устанавливает порядок обращения с государственной тайной, включая меры по предотвращению ее утечки и раскрытия.

5. Федеральный закон "О коммерческой тайне":

- Регулирует создание, использование и защиту коммерческой тайны, а также устанавливает ответственность за ее неправомерное раскрытие.

6. Федеральный закон "О персональных данных":

- Определяет правовые основы сбора, обработки и защиты персональных данных граждан.

7. Федеральный закон "Об электронной подписи":

- Устанавливает правила использования электронной подписи для обеспечения подлинности и целостности электронных документов.

8. Уголовный кодекс Российской Федерации:

- Содержит статьи, касающиеся ответственности за нарушения в сфере информационной безопасности, такие как создание и распространение вредоносных программ, незаконный доступ к информации и другие действия.

9. Трудовой кодекс Российской Федерации:

- Устанавливает правила использования информации в рабочих отношениях, включая соблюдение конфиденциальности и защиту информации организации.

10. Кодекс РФ об административных правонарушениях:

- Определяет административные наказания за нарушения законодательства в области информационной безопасности.

11. Указ Президента РФ от 17.03.2008 № 351:

- Содержит меры по обеспечению безопасности информации в информационно-телекоммуникационных сетях при международном информационном обмене.

**Ответы на контрольные вопросы**

1. Законодательные меры в области информационной безопасности необходимы для обеспечения защиты информации от незаконного доступа, утечек, разрушений или искажений. Они также направлены на обеспечение конфиденциальности, целостности и доступности информации, а также защиту от киберугроз и киберпреступлений.

2. Информационная безопасность в Российской Федерации регулируется рядом документов, включая Федеральный закон "Об информации, информационных технологиях и о защите информации", Федеральный закон "О защите конституционного права граждан на доступ к информации о деятельности государственных органов", а также нормативно-правовые акты Правительства РФ, Минкомсвязи и других ведомств.

3. Основополагающими документами в области информационной безопасности являются, например, указанные выше Федеральные законы, а также Положение о защите информации, Указ Президента РФ "О стратегии национальной безопасности Российской Федерации до 2020 года" и другие нормативные акты.