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 группы 4235

Баканина К.И.

Принял

Преподаватель Кожевников К.Д.

Казань 2024

**Часть №1**

**Цель:** Обосновать применение норм правового наказания при использовании ВПО

**Ситуации:**

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 пользователей

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.

**Анализ ситуаций:**

a) Несмотря на то, что разработчик сам не пользуется данным ПО, всё равно наносит ущерб другим компьютерам, и несет ответственность за это. По «**УК РФ Статья 273. Создание, использование и распространение вредоносных компьютерных программ**». Разработчик наказывается ограничением свободы на 4 года, либо принудительными работами на этот же срок, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

b) «**УК РФ Статья 272. Неправомерный доступ к компьютерной информации**» По данной статье, системный администратор может получить штраф, в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничение свободы на срок до четырех лет, либо принудительные работы на срок до пяти лет, либо лишение свободы на тот же срок.

c) «**УК РФ Статья 272. Неправомерный доступ к компьютерной информации**». Участник наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

d) «**УК РФ Статья 273. Создание, использование и распространение вредоносных компьютерных программ**». Хоть и не распространяли вирус, так, как его выложили на открытую платформу, это считается распространением и наказывается ограничением свободы на 4 года, либо принудительными работами на этот же срок, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

e) «**УК РФ Статья 87. Уголовная ответственность несовершеннолетних**». К несовершеннолетним, совершившим преступления, могут быть применены принудительные [меры](https://www.consultant.ru/document/cons_doc_LAW_10699/0cc4f741fbd9a23925035e7ba49750e99741734e/) воспитательного воздействия либо им может быть назначено наказание, а при освобождении от наказания судом они могут быть также помещены в специальное [учебно-воспитательное учреждение закрытого типа](https://www.consultant.ru/document/cons_doc_LAW_10699/0cc4f741fbd9a23925035e7ba49750e99741734e/).

«**УК РФ Статья 273. Создание, использование и распространение вредоносных компьютерных программ**». Хоть и не распространяли вирус, так, как его выложили на открытую платформу, это считается распространением и наказывается ограничением свободы на 4 года, либо принудительными работами на этот же срок, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

f) «**УК РФ Статья 273. Создание, использование и распространение вредоносных компьютерных программ**». Разработка вредоносных компьютерных программ, наказывается ограничением свободы на 4 года, либо принудительными работами на этот же срок, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

g) То что он за пределами РФ, не освобождает его от ответственности. «**УК РФ Статья 273. Создание, использование и распространение вредоносных компьютерных программ**». Разработка вредоносных компьютерных программ, наказывается ограничением свободы на 4 года, либо принудительными работами на этот же срок, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

**Контрольные вопросы**:

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

- Гражданская ответственность: Владелец ПО или правообладатель может предъявить иск о возмещении убытков в случае нелегального использования ПО.

- Административная ответственность: В некоторых странах нарушение законов об авторских правах на программное обеспечение влечет за собой административные штрафы.

- Уголовная ответственность: При крупном масштабе нарушения авторских прав на ПО или его незаконном распространении, лица могут быть привлечены к уголовной ответственности.

1. Как правильно лицензировать программное обеспечение?

* Определите тип лицензии
* Создайте текст лицензионного соглашения
* Распространение лицензии
* Управление лицензиями
* Защита интеллектуальной собственности
* Обновления и поддержка
* Приобретение лицензии: Приобретайте программное обеспечение только у официальных поставщиков или производителей для получения лицензии.
* Изучение лицензионного соглашения: Внимательно изучайте условия лицензионного соглашения, чтобы понимать права и обязанности пользователя.
* Соблюдение количества лицензий: Убедитесь, что количество установок программы соответствует количеству приобретенных лицензий.
* Обновление и обслуживание: Соблюдайте лицензионные требования по обновлению и поддержке программного обеспечения.

**Часть №2**

**Цель:** ознакомиться с правовой сферой в области информационной безопасности

* Документ "Конституция Российской Федерации" является одним из ключевых законодательных актов, определяющих основы государственного устройства, права и свободы граждан, а также принципы деятельности органов власти в Российской Федерации.
* Документ "Федеральный закон от 28.12.2010 № 390-ΦЗ «О безопасности»" устанавливает нормы и правила обеспечения безопасности в различных сферах жизнедеятельности граждан и государства в Российской Федерации. Он определяет меры по обеспечению конфиденциальности и защите информации, поддержание целостности информационных ресурсов, доступность услуг и данных для граждан, защиту от киберугроз, а также требования соответствия международным стандартам в области информационной безопасности. Документ является ключевым для обеспечения безопасности различных секторов общества и государства.
* Документ "Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»" устанавливает нормы и правила об обработке информации, использовании информационных технологий и защите информации в Российской Федерации.
* Документ "Закон РФ «О государственной тайне» от 21.07.1993" устанавливает правила и процедуры по определению, хранению и раскрытию государственной тайны в Российской Федерации.
* Документ "Федеральный закон «О коммерческой тайне» от 29.07.2004" устанавливает правовые основы для определения, защиты и использования коммерческой тайны в Российской Федерации.

Основные положения, которые относятся к информационной безопасности:

* Защита государственной тайны и обеспечение безопасности Российской Федерации.
* Защита информации, информационных технологий и обеспечение безопасности их использование.
* Установление порядка обработки и защиты персональных данных граждан.
* Установление правил и наказания за нарушение требований в области информационной безопасности.
* Меры по обеспечению информационной безопасности при использовании информационно-телекоммуникационных сетей и международного информационного обмена.

***Контрольные вопросы***

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

Для защиты государственных интересов, защиты персональных данных, снижения рисков для бизнеса и организаций, регулировка использования информационных технологий, международного сотрудничества,

1. Какими документами регулируется информационная безопасность в Российской Федерации?

* Федеральный закон от 27.07.2006 № 149-Ф3 “Об информации, информационных технологиях и о защите информации”
* 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»