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.4237

Фролова Е.С.

Принял

Преподаватель Кожевников К.Д.

Казань 2024

**Цель работы**

Обосновать применение норм правового наказания при использовании ВПО. Ознакомиться с правовой сферой в области информационной безопасности.

**Задание на лабораторную работу**

Часть 1

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:
3. Вы пишите на заказ программы, которые заражают компьютер и подгружают вредоносные программы. При этом самим данным программным обеспечением не пользуетесь.
4. Системный администратор некоторой известной компании без ведома устанавливал по сети всем программу для удалённого администрирования RAdmin.
5. Вы случайно распространили по сети вирус, который шифрует данные на ПК пользователей.
6. Вы не распространяли вирус, но выложили его на GitHub.
7. Вам 17 лет, ради интереса распространили вредоносное программное обеспечение.
8. Вы разработали код вредоносной программы, но ещё не воспользовались им.
9. Вы гражданин РФ и используете вредоносное программное обеспечение исключительно за пределами Российской Федерации.

Часть 2

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/

1. Охарактеризуйте данные документы с точки зрения информационной безопасности.
2. Выделите основные положения, которые относятся к информационной безопасности.

**Результат выполнения работы**

Часть 1

1. Согласно статье 273 Уголовного кодекса Российской Федерации, за разработку, распространение или использование вредоносных программ, предназначенных для нанесения ущерба работе компьютеров или средств связи, либо за создание и распространение вредоносных программ с целью совершения иных противоправных действий, предусмотрена уголовная ответственность в виде лишения свободы на срок до 3 лет.
2. Системный администратор нарушает статью 272 Уголовного кодекса Российской Федерации — Незаконный доступ к компьютерной информации. Согласно этой статье, незаконный доступ к компьютерной информации, совершённый с использованием своего служебного положения, влечёт уголовную ответственность в виде штрафа до 200 тыс. рублей, либо обязательными работами на срок до 480 часов, либо исправительными работами на срок до 2 лет, либо ограничением свободы на срок до 3 лет, либо лишением свободы на тот же срок.
3. В данной ситуации лица, распространившие вирус, могут быть привлечены к уголовной ответственности по статье 273 УК РФ "Незаконный доступ к компьютерной информации". Согласно данной статье, за совершение подобных действий лицо может быть наказано штрафом до 500 тысяч рублей, либо обязательными работами на срок до 480 часов, либо лишением свободы на срок до двух лет.
4. По Уголовному кодексу Российской Федерации, действия выкладывания вируса на GitHub могут быть квалифицированы как незаконная деятельность в области компьютерной информации (статья 273 УК РФ). По данной статье за совершение действий, целью которых является нарушение функционирования вычислительной техники, влечет уголовную ответственность в виде штрафа или лишения свободы на срок до двух лет.
5. Согласно статье 20 Уголовного кодекса Российской Федерации, лица, которые на момент совершения противоправного деяния не достигли возраста 16 лет, не несут уголовной ответственности. Однако, по указанным данным, лицу уже 17 лет, что означает, что оно достигло возраста, с которого начинается возможность привлечения к уголовной ответственности.
6. В данной ситуации, когда лицо разработало код вредоносной программы, но ещё не воспользовалось им, можно рассмотреть возможное привлечение к уголовной ответственности согласно статье 273 Уголовного кодекса Российской Федерации. Статья 273 УК РФ "Создание, использование и распространение вредоносных компьютерных программ" предусматривает наказание за создание, использование и распространение вредоносных компьютерных программ. Согласно пункту 1 статьи 273 УК РФ, создание вредоносной программы без использования или распространения её наказывается штрафом в размере до 500 тысяч, либо обязательными работами на срок до 480 часов.
7. В данной ситуации согласно статье 273.1 Уголовного кодекса Российской Федерации, гражданин РФ, использующий вредоносное программное обеспечение за пределами Российской Федерации, может привлечься к уголовной ответственности. В соответствии со статьей 273.1, внешнее использование вредоносных программ, специально предназначенных для совершения компьютерных преступлений, является уголовным преступлением.

Часть 2

* 1. Конституция Российской Федерации имеет важное значение с точки зрения информационной безопасности, так как в нём закреплены основные права и свободы граждан, а также установлены обязанности государства по защите информации и персональных данных граждан. Конституция также устанавливает основы правового регулирования в сфере информационной безопасности и кибербезопасности.

Основные положения Конституции Российской Федерации, относящиеся к информационной безопасности, включают:

* Гарантии права на конфиденциальность переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (статья 23);
* Право на неприкосновенность частной жизни (статья 24);
* Обеспечение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (статья 25);
* Защита государственных секретов, коммерческой тайны, авторских и смежных с ним прав (статья 29);
* Обеспечение безопасности информации и защита информационных ресурсов государства и общества (статья 55);
* Гарантии права на свободное получение, передачу, производство и распространение информации любым законным способом (статья 29).

2. Федеральный закон от 28.12.2010 № 390-ΦЗ «О безопасности» регулирует вопросы обеспечения безопасности в Российской Федерации. С точки зрения информационной безопасности, этот закон устанавливает нормы и правила по защите информации, в том числе персональных данных, от несанкционированного доступа, утечек и других угроз.

Основные положения закона, относящиеся к информационной безопасности, включают:

* требования к защите информации, включая установление мер по обеспечению конфиденциальности, целостности и доступности информации;
* правила обработки персональных данных и обязанности по их защите;
* установление ответственности за нарушение законодательства в области информационной безопасности;
* меры государственного контроля и надзора за обеспечением информационной безопасности.

3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» устанавливает основные принципы и правила обработки информации, информационных технологий и защите информации в Российской Федерации. Он регулирует важные аспекты информационной безопасности, такие как защита персональных данных, управление информационными ресурсами, обеспечение конфиденциальности и целостности информации и прочее.

Основные положения, относящиеся к информационной безопасности в данном документе:

* обязанность защищать информацию от несанкционированного доступа и использования;
* установление требований к организациям, обрабатывающим информацию;
* регулирование использования и защиты персональных данных;
* установление ответственности за нарушение правил обработки и защиты информации;
* создание системы мер по обеспечению информационной безопасности;
* установление понятия государственной тайны и определение процедур ее защиты.

4. Закон РФ «О государственной тайне» от 21.07.1993, имеет прямое отношение к информационной безопасности, так как регулирует сферу государственной тайны и устанавливает порядок её обеспечения. Он содержит правила и меры, направленные на защиту конфиденциальной информации от несанкционированного доступа, использования и распространения.

Основные положения, относящиеся к информационной безопасности, в данном законе включают:

* определение государственной тайны;
* установление категорий сведений, которые могут относиться к государственной тайне;
* установление порядка классификации, хранения, доступа и распространения таких сведений;
* установление ответственности за нарушение правил обращения с государственной тайной и меры по защите информации в рамках государственных органов и организаций.

5. Федеральный закон «О коммерческой тайне», представляет собой основу законодательства Российской Федерации, регулирующую вопросы конфиденциальности и защиты коммерческой информации. Он включает в себя меры по защите конфиденциальных данных, их обработке и передаче, а также устанавливает ответственность за незаконное раскрытие коммерческой тайны.

Основные положения, относящиеся к информационной безопасности в данном документе, включают в себя:

* определение понятия коммерческой тайны и её защиты;
* обязанности лиц, имеющих доступ к конфиденциальной информации;
* порядок создания и использования коммерческой тайны;
* ограничение доступа к конфиденциальной информации;
* установление сроков действия конфиденциальности;
* ответственность за нарушение законодательства о коммерческой тайне.

6. Федеральный закон "О персональных данных", имеет прямое отношение к информационной безопасности, так как регулирует сбор, хранение, использование и защиту персональных данных граждан, что является одним из основных аспектов информационной безопасности.

Основные положения, относящиеся к информационной безопасности в данном законе, включают:

* определение персональных данных и требования к их обработке;
* обязанность субъекта персональных данных предоставлять согласие на обработку его персональных данных;
* обязанность организации обеспечивать защиту персональных данных от неправомерного доступа;
* порядок уничтожения или обезличивания персональных данных после их использования;
* возможные штрафы и ответственность за нарушения закона о персональных данных.

7. Федеральный закон «Об электронной подписи», охарактеризовать с точки зрения информационной безопасности можно как законодательный акт, который регулирует использование электронной подписи в целях обеспечения безопасности электронных документов и информации. Он устанавливает правила и требования к использованию электронной подписи, чтобы гарантировать подлинность, целостность и конфиденциальность электронных данных.

Основные положения данного закона, которые относятся к информационной безопасности, включают в себя:

* установление правового статуса электронной подписи и её значение для подтверждения авторства и целостности электронных документов;
* установление требований к квалифицированным электронным подписям, которые имеют высокий уровень защиты и авторитетности;
* определение ответственности за незаконное использование электронной подписи и меры по предотвращению правонарушений;
* обеспечение защиты информации, передаваемой по электронным каналам связи, от несанкционированного доступа и изменения;
* регулирование деятельности удостоверяющих центров, которые осуществляют выдачу сертификатов на электронную подпись.

8. Документ «Уголовный кодекс Российской Федерации» от 13.06.1996 содержит информацию о преступлениях, наказуемых в соответствии с законодательством России. С точки зрения информационной безопасности данный документ содержит информацию о нарушениях и уголовных делах.

Основные положения, относящиеся к информационной безопасности в данном документе, включают:

* наказание за компьютерные преступления, такие как хакерство, кибермошенничество и нарушение неприкосновенности частной жизни через использование информационных технологий;
* защита конфиденциальной информации и персональных данных;
* установление ответственности за их утечку или незаконное использование;
* криминализация действий, направленных на нарушение работы информационных систем и сетей;
* установление мер защиты информации организаций и государственных учреждений от внешних и внутренних угроз.

9. Трудовой кодекс Российской Федерации, содержит нормативные положения, которые касаются трудовых отношений между работниками и работодателями. С точки зрения информационной безопасности, этот документ может быть важен для защиты информации о работниках, их правах и обязанностях, а также организационных мер по обеспечению безопасности на рабочем месте.

Основные положения в Трудовом кодексе, которые относятся к информационной безопасности, могут включать в себя:

* защиту конфиденциальной информации о работниках и предотвращение ее утечки;
* права и обязанности работодателей и работников по обеспечению безопасности информации на рабочем месте;
* принятие организационных мер по защите информации от несанкционированного доступа и использования;
* ответственность за нарушение правил информационной безопасности на рабочем месте.

10. Кодекс РФ об административных правонарушениях, содержит нормы и статьи, касающиеся ответственности и наказаний за нарушения административного законодательства. С точки зрения информационной безопасности, важно обратить внимание на статьи, связанные с нарушениями в области защиты информации и данных, так как безопасность информации является важным аспектом современного общества.

Основные положения, относящиеся к информационной безопасности в данном документе, могут включать:

* нарушения правил обработки и защиты информации;
* нарушения требований к защите персональных данных;
* незаконный сбор, хранение, использование и распространение информации;
* ответственность за нарушение законодательства в области информационных технологий и защиты информации.

11. Документ Указа 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» имеет прямое отношение к информационной безопасности, поскольку определяет меры по защите информации в международном информационном обмене. Документ является ключевым для обеспечения безопасности информации в стране.

Основные положения, относящиеся к информационной безопасности в данном документе, включают в себя:

* установление мер по предотвращению утечки конфиденциальной информации при использовании информационно-телекоммуникационных сетей международного информационного обмена;
* регулирование работы систем информационной безопасности в соответствии с законодательством Российской Федерации;
* установление процедур проверки и контроля за соблюдением требований по информационной безопасности;
* определение ответственности за нарушения правил и мер по обеспечению информационной безопасности;
* обеспечение сотрудничества между различными структурами и организациями в области информационной безопасности.

**Ответы на контрольные вопросы**

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

Использование нелицензионного программного обеспечения может повлечь за собой различные виды ответственности:

* гражданско-правовая ответственность: Пользователь нелицензионного программного обеспечения может быть подвержен гражданско-правовой ответственности за нарушение авторских прав владельцев программного обеспечения. Владелец программы имеет право требовать возмещения ущерба, причиненного использованием нелицензионного ПО.
* административная ответственность: Использование нелицензионного программного обеспечения может быть рассмотрено как административное правонарушение. За такие нарушения могут быть предусмотрены штрафы или другие меры административного наказания.
* уголовная ответственность: В случае совершения тяжких нарушений, например, распространения вредоносного программного обеспечения или использования программ для совершения компьютерных преступлений, лицо также может быть привлечено к уголовной ответственности.

2. Как правильно лицензировать программное обеспечение?

Для правильного лицензирования программного обеспечения рекомендуется следовать следующим рекомендациям:

* определите тип лицензии: существует несколько типов лицензий, таких как свободные, проприетарные, коммерческие и другие.
* определите условия использования: определите права и обязанности пользователей программного обеспечения, включая ограничения на использование, распространение, модификацию и т.д.
* укажите авторские права: укажите информацию об авторских правах на программное обеспечение, включая ваше имя или название компании, год создания и т.п.
* установите механизмы контроля: предусмотрите механизмы контроля использования программного обеспечения, такие как лицензионные ключи, активацию и прочее.

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

Законодательные меры в области информационной безопасности необходимы для обеспечения защиты конфиденциальности, целостности и доступности информации, а также для предотвращения киберугроз и кибератак. Они помогают устанавливать стандарты и требования к защите информации, наказывать нарушителей, регулировать использование персональных данных и обеспечивать безопасность в киберпространстве. Такие меры также способствуют повышению осведомленности населения о важности информационной безопасности и содействуют развитию сферы киберзащиты в целом.

4. Какими документами регулируется информационная безопасность в Российской Федерации?

* + - * Федеральный закон «О защите информации» — устанавливает основы регулирования обработки информации и требования к защите информации.
      * Постановление Правительства РФ «Об утверждении Правил обработки персональных данных» — содержит требования к обработке персональных данных, включая меры по обеспечению их безопасности.
      * ГОСТы и стандарты в области информационной безопасности, включая ГОСТ Р ИСО/МЭК 27001, ГОСТ Р 34.10, ГОСТ Р 34.11 и другие.

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

* Федеральный закон от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации". Этот закон устанавливает общие принципы защиты информации и информационных технологий, а также определяет правовые основы регулирования информационных отношений в России.
* Федеральный закон от 26 июля 2006 года № 149-ФЗ "О персональных данных". Этот закон устанавливает требования к обработке персональных данных граждан России, включая их сбор, хранение, использование и передачу.
* Федеральный закон от 27 июля 2006 года № 152-ФЗ "О защите конфиденциальной информации". Этот закон устанавливает правовые основы защиты конфиденциальной информации, которая составляет государственную или иную охраняемую законом тайну.

**Вывод**

Я обосновала применение норм правового наказания при использовании ВПО и ознакомилась с правовой сферой в области информационной безопасности.