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

Сафиуллин.Б.Р

Принял

Преподаватель Кожевников.К.Д

Казань 2024

**Часть 1**

**Цель работы**

Обосновать применение норм правового наказания при использовании ВПО.

**Задачи**

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.

**Результат работы**

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

Я считаю, что данное деяние наказуемо законом, так как человек распостраняет ВПО, то оно может быть использовано другими не в лучших целях, и массово или локально навредить кому-либо.

Преследуется по УК РФ Статья 273. Создание, использование и распространение вредоносных компьютерных программ.

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

Я считаю, что данное деяние наказуемо законом, так как человек распостраняет ПО без ведома компании и вообще кого-либо, то оно может быть использовано не в лучших целях: собирать персональные данные, и вообще установка ПО для распостранения по сети без ведома кого-либо неправильно. Сотрудник должен быть уволен, оштрафован.

Преследуется по УК РФ Статья 273. Создание, использование и распространение вредоносных компьютерных программ(так как программа установлена без ведома и может быть использована в нарушающих закон целях), УК РФ Статья 274.2. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования: Нарушение порядка установки, эксплуатации и модернизации в сети связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования либо несоблюдение технических условий их установки или требований к сетям связи при использовании указанных технических средств, совершенные должностным лицом или индивидуальным предпринимателем, подвергнутыми административному наказанию за деяние. А также УК РФ Статья 272. Неправомерный доступ к компьютерной информации

1. Вы случайно распространили по сети вирус, который шифрует данные на ПК пользователей

Я считаю, что данное деяние наказуемо законом, так как человек распостраняет ВПО по сети и оно используется в не в лучших целях: шифрует персональные данные ПК, соответственно получает неправомерный доступ к информации и её модернизация, установка. (за случайно бьют отчаянно). Распостранитель может получить штраф и предупреждение об удалении этого ВПО, а также может быть уголовно наказан.

Преследуется по УК РФ Статья 273. Создание, использование и распространение вредоносных компьютерных программ, УК РФ Статья 272. Неправомерный доступ к компьютерной информации:  [Неправомерный доступ](https://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/) к охраняемой законом компьютерной информации, если это деяние повлекло [уничтожение](https://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/), [блокирование](https://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/), [модификацию](https://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/) либо [копирование](https://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/) компьютерной информации.

1. Вы не распространяли вирус, но выложили его на GitHub.

Я считаю, что данное деяние наказуемо законом, так как человек распостраняет ВПО по сети с помощью платформы для пользования чужим кодом, программами и оно может использоваться в не в лучших целях. Распостранитель может получить штраф и предупреждение об удалении этого ВПО, а также может быть уголовно наказан. Платформа также может быть предупреждена, оштрафована.

Преследуется по УК РФ Статья 273. Создание, использование и распространение вредоносных компьютерных программ.

1. Вам 17 лет, ради интереса распространили вредоносное программное обеспечение.

Я считаю, что данное деяние наказуемо законом, так как человек распостраняет ВПО и оно может использоваться в не в лучших целях. Распостранитель может получить штраф и предупреждение об удалении этого ВПО, а также может быть уголовно наказан.

Преследуется по УК РФ Статья 273. Создание, использование и распространение вредоносных компьютерных программ.

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

Я считаю, что данное деяние не наказуемо законом, так как человек не нарушает ни одного закона Конституции РФ.

1. Вы гражданин РФ и используете вредоносное программное обеспечение исключительно за пределами Российской Федерации.

Согласно ст. 12 Уголовного кодекса РФ, граждане РФ, совершившие преступление вне пределов РФ подлежат уголовной ответственности по УК РФ, если совершенное ими деяние признано преступление в государстве, на территории которого было совершено, и если эти лица не были осуждены в иностранном государстве.

**Контрольные вопросы**

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

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.

1. Как правильно лицензировать программное обеспечение?

Основным документом, который определяет права и обязанности пользователя программного обеспечения, является лицензионное соглашение (licence agreement), которое прилагается к приобретенному продукту либо в виде бумажного документа, либо в электронном виде. Именно это соглашение определяет правила использования данного экземпляра продукта. По сути, лицензия выступает гарантией того, что издатель ПО, которому принадлежат исключительные права на программу, не подаст в суд на того, кто ею пользуется. Иными словами, издатель программного обеспечения ставит определенные защитные рамки по использованию его программного обеспечения.

1. Лицензирование программного обеспечения - важный аспект его разработки и распространения. Вот несколько шагов, которые вы можете следовать для правильного лицензирования ПО:

2. Определите, что вы хотите защитить: перед началом процесса лицензирования убедитесь, что вы знаете, что именно вы хотите защитить. Это может быть исходный код, документация, сколько пользователей могут использовать ваше ПО и т. д.  
 3. Выберите тип лицензии: существует много разных типов лицензий для программного обеспечения, и выбор правильного для вас будет зависеть от того, что вы хотите защитить. Открытые лицензии позволяют любому использовать, изменять и распространять ваше ПО, тогда как проприетарные лицензии ограничивают использование и дистрибуцию.  
 4.Получите юридическую помощь: подготовка лицензионного соглашения может быть сложным процессом, и ошибка может обернуться большими проблемами в будущем. Если вы не знакомы с процессом, обращение к юристу или юридической фирме, специализирующейся на лицензировании ПО, может оказаться ценным ресурсом.  
 5. Разработайте лицензионное соглашение: ваше лицензионное соглашение должно описывать, что разрешено с вашим ПО и что нет. Оно должно быть написано в простом и понятном языке и предоставлять четкое описание ограничений на использование и дистрибуцию, которые вы устанавливаете.  
6. Распространяйте лицензионное соглашение с ПО: когда ваше лицензионное соглашение готово, оно должно быть распространено вместе с вашим ПО.   
 Соблюдайте все юридические обязательства и требования: наконец, убедитесь, что вы соблюдаете все юридические требования в своем регионе касательно лицензирования и распространения вашего ПО.   
В каждом случае, рекомендуется проконсультироваться с юристом, специализирующимся на лицензировании ПО, чтобы убедиться в корректности каждого шага.

**Часть 2**

**Цель работы**

Ознакомиться с правовой сферой в области информационной безопасности.

**Задачи**

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/]( 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 работы**

1. Конституция РФ является основным законом страны, устанавливающим принципы организации и функционирования государства. В ней гарантируются основные права и свободы граждан, а также определяются принципы разделения властей и системы органов государственной власти.

2. Федеральный закон "О безопасности" № 390-ФЗ, принятый 28 декабря 2010 года, является основой регулирования вопросов обеспечения национальной безопасности Российской Федерации.   
В общих положениях установлены предмет регулирования данного закона, основные принципы обеспечения безопасности, содержание деятельности по обеспечению безопасности, государственная политика в этой области, правовая основа обеспечения безопасности, координация деятельности по обеспечению безопасности, а также международное сотрудничество в данной сфере.  
Определены полномочия федеральных органов государственной власти, функции органов государственной власти субъектов Российской Федерации и органов местного самоуправления в области обеспечения безопасности.   
Также в данном законе приведены положения о статусе Совета Безопасности, его основных задачах и функциях, составе и организации деятельности.   
Помимо этого, закон содержит ряд заключительных положений, связанных с вступлением данного закона в силу и признанием утратившими силу отдельных законодательных актов.

3. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ является одним из основных инструментов регулирования информационных отношений в Российской Федерации.   
Он задаёт основные принципы и границы взаимодействия регуляторов, правообладателей информации и пользователей. В законе определены ключевые понятия, такие как "информация", "обладатель информации", "общедоступная информация" и другие.   
Закон прописывает правила доступа к информации, включая ограничения, и ответственность за её распространение. Конкретное внимание уделено регулированию обмена информацией в интернете, включая обязанности организаторов распространения информации, операторов поисковых систем, провайдеров хостинга, новостных агрегаторов и других участников интернет-отношений.

1. Закон Российской Федерации "О государственной тайне" от 21.07.1993 N 5485-1 в его последней редакции прежде всего определяет основные понятия и принципы, а также сферу действия закона.   
   Он дает перечень сведений, которые можно отнести к государственной тайне и которые не могут быть засекречены.   
   Законом устанавливается порядок отнесения сведений к государственной тайне, их засекречивания, а также рассекречивания.   
   Закон описывает, как управлять сведениями, которые составляют государственную тайну, включая их передачу между органами государственной власти и даже их передачу другим государствам или международным организациям.   
   В нем указываются органы, ответственные за защиту государственной тайны, а также правила предоставления, прекращения и ограничения доступа к государственной тайне.   
   Закон о государственной тайне также регламентирует ответственность за нарушения закона, финансирование мероприятий по защите государственной тайны и контроль за этой защитой.
2. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ регулирует отношения, связанные с защитой информации, которую организации или индивидуальные предприниматели рассматривают как коммерческую тайну.   
   Основные понятия, детализированные в законе, включают определение самого понятия "коммерческая тайна", а также классификацию информации, которая может и не может быть отнесена к коммерческой тайне.  
   Закон определяет правила относительно отнесения информации к коммерческой тайне, ее предоставления, защиты и возможных штрафов за нарушение этих правил.   
   Он также обсуждает особенности защиты коммерческой тайны в рамках трудовых отношений и при передаче информации между сторонами.  
   Специальное внимание уделено обязанностям предприятий перед государством в отношении предоставления информации, которая может считаться коммерческой тайной.
3. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ закрепляет правовые основы защиты персональных данных граждан, обеспечивает защиту их прав на неприкосновенность частной жизни, личной и семейной тайны в связи с обработкой персональных данных, прав на свободное распоряжение своими персональными данными.  
     
   Закон регулирует отношения, возникающие при обработке персональных данных, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.  
     
   Основные принципы, описанные в законе, включают обработку персональных данных на законной и справедливой основе; обработку персональных данных, ограниченную достижением конкретных, заранее определенных и законных целей; несовместимость с целями сбора персональных данных.  
     
   Важной частью закона являются права субъектов персональных данных. Это включает право на доступ к своим персональным данным, право на исправление, блокирование или уничтожение своих персональных данных, если они неполные, устаревшие, неточные, незаконно получены или не являются необходимыми для заявленной цели обработки, а также право на защиту своих прав и законных интересов, включая защиту прав в суде и обжалование действий или бездействия оператора.

Закон также содержит требования к операторам обработки данных, включая обязательства по обеспечению безопасности персональных данных.

1. Федеральный закон "Об электронной подписи" от 06.04.2011 N 63-ФЗ регулирует отношения, возникающие при создании и использовании электронных подписей в России.  
   Закон устанавливает определения таких понятий, как электронная подпись, простая и усиленная электронная подписи, средство электронной подписи и удостоверяющий центр.  
   Принципы использования электронной подписи определяются на основе закона. Они включают, но не ограничиваются, основами использования электронной подписи, обязательствами участников электронного взаимодействия при использовании усиленной электронной подписи, а также признанием квалифицированных электронных подписей.  
   Особое внимание в законе уделяется нормам об использовании разных видов электронной подписи для различных групп пользователей. Это включает физических лиц, юридических лиц, государственных органов, органов местного самоуправления и других организаций.  
   Закон регулирует процессы создания, аккредитации и проверки удостоверяющих центров, в которых производится выдача сертификатов ключей подписи. Кроме того, он определяет положения о третьих доверенных лицах, которые помогают в проверке электронных подписей.

8. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ является законодательством, которое регулирует уголовное законодательство в России. Он был принят Государственной Думой 24 мая 1996 года и одобрен Советом Федерации 5 июня 1996 года.   
  
Документ содержит различные статьи, которые определяют уголовные преступления и назначают соответствующие уголовные наказания. Он обновляется по мере необходимости для учёта изменяющихся общественных условий и норм.

9. "Трудовой кодекс Российской Федерации" от 30 декабря 2001 года N 197-ФЗ - это документ, регулирующий трудовые отношения в Российской Федерации. Трудовой Кодекс включает в себя регулирование всех видов трудовых отношений, связанных с выполнением оплачиваемой работы.  
Кодекс был принят Государственной Думой 21 декабря 2001 года и одобрен Советом Федерации 26 декабря 2001 года.

10. "Кодекс Российской Федерации об административных правонарушениях" от 30 декабря 2001 года N 195-ФЗ (ред. от 25 декабря 2023) был принят Государственной Думой 20-го декабря 2001 года и одобрен Советом Федерации 26-го декабря 2001 года.  
  
Этот документ является основным нормативно-правовым актом, который регулирует вопросы, связанные с административной ответственностью за совершение административных проступков на территории Российской Федерации.   
  
В качестве санкций за совершение административного правонарушения закон может предусматривать штрафы, административный арест, общественные работы и другие виды наказаний.

11. Указ Президента РФ от 17.03.2008 N 351 (ред. от 22.05.2015) "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" был создан для регулирования и обеспечения безопасности информации при использовании телекоммуникационных сетей.  
  
Среди основных положений указа:  
  
1. Запрет на подключение информационных систем и сетей, содержащих информацию, составляющую государственную или служебную тайну, к сетям международного информационного обмена без использования специальных средств защиты информации.  
2. Обязательное использование государственными органами сертифицированных средств защиты информации для защиты общедоступной информации в сетях международного информационного обмена.  
3. Размещение технических средств, подключенных к информационно-телекоммуникационным сетям международного информационного обмена, в помещениях, предназначенных для ведения переговоров, обсуждающих вопросы, содержащие сведения, составляющие государственную тайну, разрешается только при наличии соответствующего сертификата.  
Указ также предусматривает обязательность исполнения этих требований для всех операторов информационных систем, владельцев информационно-телекоммуникационных сетей и средств вычислительной техники.

**Контрольные вопросы**

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

Законодательные меры в области информационной безопасности жизненно важны для защиты данных и информационных систем от нежелательных угроз. Это включает в себя защиту от киберпреступлений, вирусов, вредоносного ПО, а также методов нелегального доступа. Они также могут помочь обеспечить конфиденциальность, целостность и доступность информации.

2. Какими документами регулируется информационная безопасность в Российской Федерации?

В Российской Федерации информационная безопасность регулируется несколькими ключевыми документами, включая:  
- Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ  
- Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ  
- Указ Президента РФ от 17.03.2008 N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»

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

Основополагающие документы в области информационной безопасности включают:

- Федеральный закон "Об информации, информационных технологиях и о защите информации"  
- Федеральный закон "О персональных данных"  
- Концепция национальной безопасности Российской Федерации  
- Доктрина информационной безопасности Российской Федерации  
- Указ Президента РФ «О стратегии национальной безопасности Российской Федерации»  
- Нормативные документы Федеральной службы по техническому и экспортному контролю.

Вывод: Изучили нормы права в сфере информационной безопасности.