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 4233

Галиев Р.Р.

Принял

Преподаватель Кожевников К.Д.

Казань 2024

**Часть №1**

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

**Выполнение работы:**

Согласно Уголовному кодексу Российской Федерации, ответственность за различные ситуации, описанные в вопросе, будет иметь следующий характер:  
  
a) В данной ситуации, когда человек пишет на заказ программы, которые заражают компьютеры и загружают вредоносные программы, он несет ответственность согласно статье 273.1 УК РФ за:  
- Производство, хранение, передачу или продажу программ для ЭВМ, предназначенных для совершения преступлений.  
  
b) Системный администратор в данном случае, устанавливавший программу RAdmin без ведома, может быть привлечен к ответственности по статье 273 УК РФ за:  
- Создание, использование и распространение компьютерных программ и тайнописей, предназначенных для несанкционированного вторжения в вычислительную машину, сеть или компьютерную информацию.  
  
c) Человек, случайно распространивший вирус шифрования данных по сети, будет привлечен к ответственности по статье 273.1 УК РФ за:  
- Производство, хранение, передачу или продажу программ для ЭВМ, предназначенных для создания вредоносных электронных образов.  
  
d) Размещение вредоносного кода на GitHub может быть квалифицировано как деяние, предусмотренное статьей 273.1 УК РФ о производстве, хранении, передаче или продаже вредоносных программ.  
  
e) В случае 17-летнего лица распространение вредоносного ПО также может повлечь за собой уголовную ответственность согласно статье 273.1 УК РФ.  
  
f) Создание кода вредоносной программы, но без фактического использования его, может также влечь привлечение к уголовной ответственности по тем же статьям.  
  
g) Использование вредоносного ПО за пределами Российской Федерации также может привлечь к уголовной ответственности в зависимости от характера этих действий и законодательства той страны, где они были совершены.

**Контрольные вопросы**

1. Виды ответственности за использование нелицензионного программного обеспечения включают:   
   - Гражданско-правовую ответственность, когда правообладатель имеет право требовать возмещения ущерба, причиненного использованием нелицензионного ПО.  
   - Административную ответственность, в случае нарушения законодательства в области авторских прав.  
   - Уголовную ответственность, если использование нелицензионного ПО расценивается как преступление, например, по статье 146 УК РФ (нарушение авторских и смежных прав).  
    
2. Для правильной лицензировки программного обеспечения следует соблюдать следующие рекомендации:  
   - Приобретать программное обеспечение у официальных поставщиков или производителей.  
   - Внимательно читать и понимать лицензионное соглашение перед покупкой или использованием ПО.  
   - Убедиться, что количество купленных лицензий соответствует количеству устройств или пользователей, на которых будет использоваться ПО.  
   - Периодически проверять и обновлять лицензии в соответствии с законодательством и соглашением с правообладателем.  
   - Соблюдать условия использования ПО, указанные в лицензионном соглашении, включая ограничения по установке и копированию ПО.  
   - В случае сомнений или вопросов по лицензированию, обращаться к специалистам или юристам, специализирующимся на интеллектуальной собственности и лицензировании программного обеспечения.

**Часть №2**

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

**Выполнение работы:**

1. Федеральный закон от 28.12.2010 № 390-ΦЗ «О безопасности»:

*Федеральный закон от 28.12.2010 № 390-ФЗ "О безопасности" устанавливает общие принципы государственной политики в области обеспечения безопасности Российской Федерации. В этом законе определяются основные направления деятельности в области безопасности, включая защиту государственного суверенитета, территориальной целостности, независимости и конституционного строя, а также обеспечение обороноспособности страны.*

*Статья 4 данного закона устанавливает, что государственная политика в области обеспечения безопасности направлена на пресечение угроз национальной безопасности, обеспечение прав и свобод человека и гражданина, защиту интересов общества и государства от противоправного вмешательства в их деятельность. Она также направлена на предотвращение внешних и внутренних угроз безопасности, осуществление защиты государственной границы, обеспечение безопасности личности, общества и государства.*

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»:

*Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" устанавливает основные нормы и правила в области информации, информационных технологий и защиты информации. Он регулирует правовые отношения, связанные с сбором, обработкой, хранением, передачей и использованием информации, а также определяет порядок обеспечения безопасности информации.*

*В этом законе содержатся требования к защите прав граждан и организаций при обработке и передаче их персональных данных, а также устанавливаются обязанности организаций по обеспечению конфиденциальности информации. Закон также определяет правила использования информационных технологий, включая электронную подпись и электронный документ.*

*В статье 6 данного закона уточняются общие принципы законодательного регулирования информационных отношений, включая принципы законности, свободы информации, равноправия участников информационных отношений, обеспечения конфиденциальности информации, защиты прав субъектов информационных отношений и прочие принципы, необходимые для обеспечения правопорядка в сфере информации и информационных технологий.*

1. Закон РФ «О государственной тайне» от 21.07.1993:

*Закон РФ "О государственной тайне" от 21.07.1993 года устанавливает правовые основы для определения государственной тайны, ее режима и защиты. Этот закон определяет процедуру классификации сведений как государственной тайны, устанавливает порядок доступа к такой информации, а также устанавливает ответственность за ее незаконное распространение или использование. Закон "О государственной тайне" также устанавливает порядок создания, использования и хранения государственных секретов, а также определяет категории сведений, которые могут быть отнесены к государственной тайне. Важной частью данного закона является определение органов, уполномоченных на принятие решений о классификации информации как государственной тайны и осуществление контроля за соблюдением режима ее секретности. В статье 5 указанного закона содержится норма, которая определяет порядок и условия классификации информации как государственной тайны. В данной статье указывается, что установление степени секретности информации и принятие решения о ее классификации осуществляется компетентными органами в соответствии с установленными законом процедурами.*

1. Федеральный закон «О коммерческой тайне» от 29.07.2004:

*Федеральный закон "О коммерческой тайне" от 29.07.2004 года устанавливает правовые основы для защиты коммерческой тайны – информации, которая не общедоступна и имеет экономическую ценность. Закон определяет понятие коммерческой тайны, права и обязанности ее обладателей, а также порядок защиты такой информации от незаконного использования или раскрытия. В соответствии с данным законом, сведения могут быть признаны коммерческой тайной, если они обладают новизной, промышленной или иной экономической значимостью, а их обладатель принял необходимые меры по сохранению их конфиденциальности. Закон "О коммерческой тайне" также определяет ответственность за нарушение права на коммерческую тайну, включая возможность реализации требований о запрете использования или раскрытия такой информации. Статья 4 данного закона устанавливает критерии, по которым информация может быть признана коммерческой тайной. В частности, в данной статье указывается, что сведения, составляющие коммерческую тайну, должны быть секретными, иметь коммерческую ценность и не быть общедоступными. Кроме того, поведение и нормы деловой этики в соответствии с данным законом также регулируются вопросы конфиденциальности об источниках информации и других аспектов коммерческой тайны.*

1. Федеральный закон «О персональных данных» от 27.07.2006:  
    *Федеральный закон "О персональных данных" от 27.07.2006 года регулирует сбор, обработку и хранение персональных данных граждан. Целью этого закона является защита прав человека и гражданина при обработке и использовании их персональных данных, а также определение ответственности за нарушения в этой сфере. Закон устанавливает требования к соблюдению принципов обработки персональных данных, включая законность, обоснованность и справедливость.*

*Основные положения закона "О персональных данных" касаются определения понятия персональных данных, прав граждан на защиту и доступ к своим данным, обязанности субъектов обработки персональных данных по обеспечению их конфиденциальности и безопасности. Закон также устанавливает требования к организациям, осуществляющим обработку персональных данных, в том числе к разработке внутренних документов и мерам по защите информации. Статья 6 данного закона устанавливает обязанности субъектов персональных данных при их обработке. В этой статье прописаны основные принципы обработки персональных данных, которые включают законность и справедливость обработки, ограничение обработки данных только по предназначению, соблюдение конфиденциальности и другие важные положения для обеспечения защиты прав граждан на конфиденциальность и безопасность их личных данных.*

1. Федеральный закон «Об электронной подписи» от 06.04.2011:  
   *Федеральный закон "Об электронной подписи" от 06.04.2011 года регулирует использование электронной подписи как способа подтверждения подлинности электронных документов и согласий. Целью данного закона является содействие развитию информационного общества, обеспечение безопасности и защиты информации при использовании электронной подписи, а также создание правовых основ для электронного взаимодействия граждан, организаций и государственных органов.*

*Закон "Об электронной подписи" устанавливает требования к процедурам создания, использования и проверки электронных подписей, а также определяет основания и порядок признания их действительными. Основными принципами действия электронной подписи в рамках данного закона являются надежность, достоверность и невозможность отрицания использования подписи.  
 Статья 3 данного закона определяет понятие электронной подписи и ее виды. В этой статье содержатся основные определения, которые являются основой для правильного понимания и применения закона, включая такие термины, как "электронный документ", "держатель ключа подписи" и другие, необходимые для корректного использования электронной подписи в цифровом пространстве.*

1. «Уголовный кодекс Российской Федерации» от 13.06.1996:

*Федеральный закон "Уголовный кодекс Российской Федерации" от 13.06.1996 устанавливает нормы уголовного права, определяющие составы преступлений и наказания за их совершение. В соответствии со статьей 105 УК РФ, устанавливаются наказания за убийство, в зависимости от обстоятельств и мотивов преступления. Закон также регулирует ответственность за кражу (статья 158 УК РФ), мошенничество (статья 159 УК РФ), насилие (статья 116 УК РФ) и другие деяния, квалифицируемые как преступления. Уголовный кодекс содержит нормы о мерах принудительного воздействия (статьи 53-73 УК РФ) и ограничениях права на отдельные виды деятельности для осужденных. Закон направлен на обеспечение законности, защиту общественного порядка и безопасности граждан, а также на предотвращение и наказание преступлений. В целом, "Уголовный кодекс Российской Федерации" является основополагающим документом в области уголовного права, определяющим преступные действия и соответствующие им уголовные наказания.*

1. «Трудовой кодекс Российской Федерации» от 30.12.2001:

*Федеральный закон "Трудовой кодекс Российской Федерации" от 30.12.2001 устанавливает правовые основы регулирования трудовых отношений между работодателем и работником. В соответствии со статьей 17 ТК РФ, работник имеет право на оплату труда в срок и согласно установленным нормам и условиям трудового договора или коллективного договора. Закон регулирует порядок заключения трудовых договоров, условия труда, рабочее время, отпуска, увольнение и другие аспекты трудовой деятельности. "Трудовой кодекс" содержит нормы о гарантиях и компенсациях при трудовой деятельности, охране труда, соблюдении рабочего распорядка и трудовой дисциплине. Закон устанавливает права и обязанности работников и работодателей, а также механизмы разрешения трудовых споров и конфликтов. "Трудовой кодекс Российской Федерации" направлен на обеспечение справедливости и социальной защиты трудящихся, а также на содействие стабильным и эффективным трудовым отношениям в стране.*

1. Кодекс РФ об административных правонарушениях:

*Кодекс Российской Федерации об административных правонарушениях регулирует порядок ответственности за совершение административных правонарушений. В соответствии с статьей 2.1 КоАП РФ, административным правонарушением признается деяние, предусмотренное законом как правонарушение и наказуемое административным наказанием. Кодекс устанавливает виды административных наказаний, такие как штрафы, административный арест, лишение специальных прав, административное выдворение и другие. В законе прописаны процедуры вынесения постановлений о наложении административного наказания, права и обязанности субъектов административного процесса. Кодекс также определяет сроки и процедуры обжалования решений о наложении административного наказания, а также меры по применению административного наказания к юридическим лицам. Кодекс об административных правонарушениях направлен на обеспечение законности, порядка и общественной безопасности, а также на предотвращение и наказание нарушений административного характера.*

1. 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»:  
    *Указ Президента РФ от 17.03.2008 № 351 (ред. от 22.05.2015) был принят для обеспечения информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена. В указе устанавливаются меры по защите государственных информационных ресурсов от угроз, связанных с электронным шпионажем, кибератаками и другими формами враждебной деятельности в киберпространстве. Документ также регламентирует взаимодействие органов государственной власти, органов местного самоуправления, общественных организаций и частных лиц в области информационной безопасности. Президентским указом утверждаются меры по обеспечению защиты информационных ресурсов и критической информационной инфраструктуры страны от угроз в сети интернет. Указ также содержит положения о контроле и мониторинге информационных потоков, организации инцидентного реагирования в случае кибератак и других событий, угрожающих информационной безопасности России. Этот документ призван обеспечить защиту национальных интересов и союзников в киберпространстве и предотвратить потенциальные угрозы для информационной безопасности государства.*

**2. Охарактеризуем данные документы с точки зрения информационной безопасности:**  
  
*- Конституция Российской Федерации: Определяет основные принципы государственного устройства и защиты прав и свобод граждан, включая право на конфиденциальность персональных данных и информационную безопасность.  
  
- Федеральный закон "О безопасности": Устанавливает общие принципы обеспечения безопасности в различных сферах деятельности, включая информационную безопасность.  
  
- Федеральный закон "Об информации, информационных технологиях и о защите информации": Регулирует обработку, хранение и передачу информации, в том числе устанавливает требования к защите информации.  
  
- Закон РФ "О государственной тайне": Определяет порядок обращения с информацией, составляющей государственную тайну, и устанавливает меры по ее защите.  
  
- Федеральный закон "О коммерческой тайне": Регулирует правовой статус коммерческой тайны и устанавливает порядок ее защиты.  
  
- Федеральный закон "О персональных данных": Регулирует сбор, хранение и обработку персональных данных граждан, а также устанавливает требования к их защите.  
  
- Федеральный закон "Об электронной подписи": Устанавливает правовой статус и порядок применения электронной подписи для обеспечения целостности и подлинности электронных документов.  
  
- Уголовный кодекс РФ: Содержит статьи, касающиеся киберпреступлений и наказания за нарушения в области информационной безопасности.  
  
- Трудовой кодекс РФ: Устанавливает правила по обеспечению конфиденциальности информации, включая правила обращения с информацией работодателя.  
  
- Кодекс РФ об административных правонарушениях: Регулирует ответственность за нарушения в области информационной безопасности.  
  
- Указ Президента РФ от 17.03.2008 № 351: Направлен на обеспечение информационной безопасности России в киберпространстве и установление мер по защите информационных ресурсов.*

**3. Выделим основные положения, относящиеся к информационной безопасности:**

*- Конституция РФ: Гарантирование защиты частной жизни, документов, переписки, телефонных разговоров и других сообщений.*

*- Федеральный закон "О безопасности": Положения о защите информационной безопасности в рамках обеспечения безопасности государства.*

*- Федеральный закон "Об информации, информационных технологиях и о защите информации": Установление требований к защите информации, включая меры по предотвращению утечки и несанкционированному доступу.*

*- Закон РФ "О государственной тайне": Регулирование порядка обращения с государственной тайной и установление мер по ее защите.*

*- Федеральный закон "О коммерческой тайне": Установление правовых норм по обеспечению конфиденциальности коммерческой информации.*

*- Федеральный закон "О персональных данных": Установление правил обработки и защиты персональных данных граждан.*

*- Федеральный закон "Об электронной подписи": Регулирование использования электронных подписей для обеспечения безопасности электронных документов.*

*- Уголовный кодекс РФ: Особые статьи о наказании за совершение киберпреступлений и нарушения в области информационной безопасности.*

*- Трудовой кодекс РФ: Установление правил обработки и защиты информации работодателя.*

*- Кодекс РФ об административных правонарушениях: Установление ответственности за нарушения в области информационной безопасности.*

*- Указ Президента РФ от 17.03.2008 № 351: Утверждение мер по обеспечению информационной безопасности Российской Федерации и защите информационных ресурсов от угроз в киберпространстве.*

**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?

**Ответы на контрольные вопросы:**  
1. Законодательные меры в области информационной безопасности нужны для обеспечения защиты информации от несанкционированного доступа, утечек, повреждений или уничтожения. Они также направлены на обеспечение конфиденциальности данных, защиту персональной информации граждан, предотвращение киберугроз и киберпреступлений, а также гарантирование целостности и доступности информационных ресурсов.  
  
2. Информационная безопасность в Российской Федерации регулируется следующими документами:  
- Конституция Российской Федерации;  
- Федеральные законы (например, "О безопасности", "Об информации, информационных технологиях и о защите информации", "О персональных данных", и др.);  
- Указы Президента РФ и Правительства РФ;  
- Нормативные акты по информационной безопасности от Минкомсвязи России и других государственных органов;  
- Международные и межгосударственные документы в области кибербезопасности.  
  
3. Основополагающие документы в области информационной безопасности, известные мне, включают:  
- Конституция Российской Федерации;  
- Федеральный закон "О безопасности";  
- Федеральный закон "Об информации, информационных технологиях и о защите информации";  
- Федеральный закон "О персональных данных";  
- Федеральный закон "Об электронной подписи";  
- Указ Президента РФ от 17.03.2008 № 351 о мерах по обеспечению информационной безопасности России в киберпространстве.