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

Шевчук О.А.

Принял

Преподаватель Кожевников К.Д.

Казань 2024

**Часть №1**

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

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

В данном примере четко указано что разработчик занимается созданием и распространением вредоносного ПО. Если заказ создан в законных целях и программа не будет использована с целью нанесения вреда гражданам донное действие является законным, но должно быть регламентировано компанией.

В случае нанесения вреда, по статье 273.1 УК РФ, распространение или использование вредоносных компьютерных программ - наказываются ограничением свободы или другими мерами.

Таким образом, лицо, которое пишет на заказ вредоносные программы, может быть привлечено к уголовной ответственности за совершение указанных действий.

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

В случае если администратор уничтожил, модифицировал или заблокировал информацию по статье 272 УК РФ ему грозит штраф либо исправительные работ, либо ограничение свободы.

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

По статье 273.1 УК РФ, распространение или использование вредоносных компьютерных программ - наказываются ограничением свободы или другими мерами. Но так как лицо непреднамеренно распространило вирус то скорее всего, уголовная ответственность не грозит.

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

В данной ситуации выкладывание в сеть вирусного ПО является преступлением, и попадает под статью о создании вредоносного ПО.

Владельцы площадки, хранящей вредоносный код, также могут быть привлечены к ответственности за распространение вредоносного ПО.

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

Распространение вируса было намеренным, соответственно не законным. В случае с несовершеннолетним, которому на момент совершения деяния исполнилось 16 лет, наказание может быть назначено с учетом его возраста и иных обстоятельств дела.

**Вы разработали код вредоносной программы, но eще не воспользовались им.**

Действия, описанные в примере, являются созданием вредоносной компьютерной программой, соответственно попадают под статью 273 УК РФ. При этом пример подразумевает что злоумышленник собирается воспользоваться программой.

Также данную ситуацию можно рассмотреть, как и ситуацию а, если код создан в законных целях и является заказом для использования в законных целях. Если программа не будет использована с целью нанесения вреда гражданам донное действие является законным, но должно быть регламентировано компанией.

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

Если гражданин находится за границей, но использует вредоносное ПО манипулируя данными российских компаний и пользователей к нему должны быть применены меры предписанные УК РФ.

В случае если же пользователь наносит вред не российским данным он понесет ответственность в соответствии с законами страны гражданам и компаниям которых был нанесен ущерб. Если в стране, в которой находится злоумышленник есть закон, запрещающий использование вредоносных программ он также может быть наказан в соответствии с документом.

**Ответы на контрольные вопросы:**

1. Виды ответственности за использование нелицензионного программного обеспечения:

- Гражданско-правовая ответственность, предусматривает возможные штрафы или выплаты компенсаций владельцу программного обеспечения за незаконное использование.

-Административная ответственность: административные штрафы, замечания или другие меры, наложенные уполномоченными органами.

-Уголовная ответственность в случае умышленного использования пиратского программного обеспечения с целью получения материальной выгоды.

2. Для правильного лицензирования программного обеспечения необходимо следовать следующим шагам:

- Приобрести лицензионное соглашение у владельца программного обеспечения. В соглашении должны быть четко определены правила использования и лицензирования программы.

- Удостовериться, что количество приобретенных лицензий соответствует количеству пользователей программы, а также типу использования (коммерческое, личное и т. д.).

- Соблюдать условия лицензионного соглашения, включая запрет на копирование, распространение и изменение программного обеспечения без разрешения владельца.

- Регулярно обновлять лицензии и следить за сроками действия лицензионного соглашения.

**Часть №2**

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

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» определяет основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством Российской Федерации, полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления в области безопасности, а также статус Совета Безопасности Российской Федерации.
3. Настоящий Федеральный закон («Об информации, информационных технологиях и о защите информации») регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

1. Закон РФ «О государственной тайне» регулирует отношения, связанные с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой государственной тайны в интересах обеспечения безопасности Российской Федерации.
2. Федеральный закон «О коммерческой тайне» регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.
3. Законом «О персональных данных» регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, иными муниципальными органами, юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий, совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и доступ к таким персональным данным.
4. Федеральный закон «Об электронной подписи» регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами.
5. Уголовный кодекс Российской Федерации (УК РФ) — основной источник уголовного права и единственный нормативный акт, устанавливающий преступность и наказуемость деяний на территории Российской Федерации.
6. Целями трудового законодательства являются установление государственных гарантий трудовых прав и свобод граждан, создание благоприятных условий труда, защита прав и интересов работников и работодателей.

Основными задачами трудового законодательства являются создание необходимых правовых условий для достижения оптимального согласования интересов сторон трудовых отношений, интересов государства, а также правовое регулирование трудовых отношений и иных непосредственно связанных с ними отношений по:

* организации труда и управлению трудом;
* трудоустройству у данного работодателя;
* подготовке и дополнительному профессиональному образованию работников непосредственно у данного работодателя;

1. Задачами законодательства об административных правонарушениях являются защита личности, охрана прав и свобод человека и гражданина, охрана здоровья граждан, санитарно-эпидемиологического благополучия населения, защита общественной нравственности, охрана окружающей среды, установленного порядка осуществления государственной власти, общественного порядка и общественной безопасности, собственности, защита законных экономических интересов физических и юридических лиц, общества и государства от административных правонарушений, а также предупреждение административных правонарушений.
2. Указ президента о мерах по обеспечению информационной безопасности касается обеспечения информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей, включая Интернет. Указ устанавливает ограничения на подключение информационных систем к международным сетям, требования к защите информации, используемой государственными органами, и правила размещения технических средств.

**Ответы на контрольные вопросы:**

1. Законодательные меры в области информационной безопасности существуют для защиты информации и информационных ресурсов от несанкционированного доступа, утечек, порчи или уничтожения.
2. В Российской Федерации информационная безопасность регулируется рядом законодательных актов, включая Федеральный закон «О защите информации», Федеральный закон «Об информации, информационных технологиях и о защите информации».
3. В Российской Федерации основополагающие документы в области информационной безопасности включают:

1. 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.

2. 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.

3. 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:** Законодательство Российской федерации обеспечивает безопасность информационных ресурсов. Также в нем рассмотрено понятие «вредоносное ПО» и ограничения по его использованию.