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.4233

Загумёнов А.О.

Преподаватель

Кожевников К. Д.

Казань 2024

**Часть №1**

**Цель на лабораторную работу**

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

**Задание на лабораторную работу**

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 выполнения работы**

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

Ответ: В данной ситуации вы оказываете прямое содействие в распространении вредоносных программ, что может быть квалифицировано как действие, направленное на нарушение функционирования компьютерных систем. В данном случае вы не используете сами вредоносные программы, но их создание и распространение уже является преступлением. Распространение программ, которые заражают компьютеры и подгружают вредоносные программы, может быть квалифицировано как нарушение целостности компьютерной информации. В данном случае несет ответственность человек, который написал на заказ такие программы. (Cтатья 273 УК РФ - Незаконный доступ к компьютерной информации.)

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

Ответ: Системный администратор, который устанавливал программу RAdmin без ведома компании, может быть привлечен к уголовной ответственности за незаконный доступ к компьютерной информации. Установка программы для удаленного администрирования без согласия компании может быть расценена как незаконный доступ к компьютерной информации. Виновным будет считаться системный администратор. (Статья 272 УК РФ - Нарушение неприкосновенности частной жизни.)

c) Вы случайно распространили по сети вирус, который шифрует данные на ПК пользователей

Ответ: Распространение вируса, который шифрует данные на ПК пользователей, также может быть признано преступлением согласно статье. Распространение вируса, который шифрует данные на ПК пользователей, также может быть преступным деянием согласно статье 273.1 УК РФ. Ответственность несет лицо, которое случайно распространило вредоносное ПО

d) Вы не распространяли вирус, но выложили его на GitHub.

Ответ: В данной ситуации, когда вы разместили вирус на GitHub, возникает серьезное нарушение информационной безопасности. Размещение вредоносного программного обеспечения на публичном ресурсе может привести к нежелательным последствиям, таким как инфицирование компьютеров пользователей, утрата данных и организационные проблемы. Статья 273.2 УК РФ - "Создание, использование и распространение вредоносных компьютерных программ". При наличии доказательств размещения вредоносного программного обеспечения на GitHub, лицо может быть обвинено в создании или распространении вредоносных компьютерных программ.

e) Вам 17 лет, ради интереса распространили вредоносное программное обеспечение.

Ответ: В случае, если вам 17 лет и вы распространили вредоносное программное обеспечение ради интереса, вы все равно можете быть привлечены к уголовной ответственности в соответствии с законодательством Российской Федерации. Возможно, в вашем случае в силу возраста будут применяться особые условия или меры ответственности, предусмотренные для лиц несовершеннолетнего возраста. (Статья 274 УК РФ - Нарушение правил пользования электронными или информационными ресурсами.)

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

Ответ: Разработка кода вредоносной программы в соответствии с уголовным законодательством может рассматриваться как уголовное преступление, независимо от того, был ли код использован. Вам может быть предъявлено обвинение в совершении преступления, предусмотренного статьей 272 УК РФ - Незаконный доступ к компьютерной информации.

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

Ответ: В случае использования вредоносного программного обеспечения за пределами Российской Федерации, тем не менее, вам как гражданину РФ может быть применено уголовное преследование согласно законодательству своей страны. Как гражданину РФ вам может быть предъявлено обвинение в совершении преступления по законам России в случае, если ваши действия могут быть квалифицированы как преступление в РФ. (Статья 273.2 УК РФ - Создание, использование и распространение вредоносных компьютерных программ.

**Контрольные вопросы**

1. Виды ответственности за использование не лицензионного программного обеспечения могут включать:

- Гражданско-правовая ответственность: лицензионное соглашение является договором, который устанавливает условия использования программного обеспечения. Несоблюдение условий лицензионного соглашения может привести к гражданско-правовой ответственности, включая уплату возмещения ущерба.

- Административная ответственность: в зависимости от законодательства страны, использование нелицензионного программного обеспечения может быть рассматриваться как административное правонарушение с предусмотренными штрафами.

- Уголовная ответственность: в некоторых случаях использование нелицензионного программного обеспечения может быть квалифицировано как преступление, что влечет за собой уголовную ответственность.

2. Для правильной лицензировки программного обеспечения следует выполнить следующие шаги:

- Ознакомьтесь с лицензионным соглашением программного обеспечения. В нем указаны условия использования, правила лицензирования, ограничения и другая необходимая информация.

- Приобретите лицензию у авторизованного поставщика программного обеспечения. Обратитесь к официальному дистрибьютору или производителю программы для заключения лицензионного договора.

- Установите программное обеспечение в соответствии с условиями лицензионного соглашения. Обеспечьте корректную установку и активацию продукта.

- Осуществляйте контроль за лицензии: следите за их сроком действия, убедитесь, что количество используемых копий соответствует лицензионным условиям.

Правильная лицензировка программного обеспечения является важным аспектом информационной безопасности и соблюдения законодательства в области использования программного обеспечения.

**Часть №2**

**Цель на лабораторную работу**

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

**Задание на лабораторную работу**

1. Ознакомьтесь со следующими документами.
2. Охарактеризуйте данные документы с точки зрения информационной безопасности
3. Выделите основные положения, которые относятся к информационной безопасности

**Результат выполнения работы**

1) Конституция Российской Федерации

Конституция Российской Федерации является основным законодательным актом страны, который определяет основные принципы государственного устройства, гарантирует права и свободы граждан. С точки зрения информационной безопасности, данная Конституция устанавливает важные положения, связанные с защитой информации и конфиденциальности персональных данных. Право граждан на конфиденциальность персональных данных. Обязанность государства обеспечивать защиту информации, связанной с правами человека и гражданина. Гарантии защиты информации от несанкционированного доступа и использования. Конституция Российской Федерации содержит важные нормы и принципы, направленные на обеспечение информационной безопасности, защиту персональных данных и обеспечение конфиденциальности информации в целом. Она является основой для разработки законов и нормативных актов, регулирующих информационные отношения в обществе и обеспечивающих защиту информации от угроз и нарушений.

2) Федеральный закон от 28.12.2010 № 390-ΦЗ «О безопасности»

Федеральный закон от 28.12.2010 № 390-ΦЗ «О безопасности» представляет собой важный юридический акт, направленный на обеспечение безопасности в различных сферах деятельности, включая информационную безопасность. Данный закон устанавливает нормы и правила, направленные на предотвращение угроз безопасности, в том числе в области информационных технологий и обработки информации. Федеральный закон "О безопасности" играет важную роль в обеспечении информационной безопасности в России, обеспечивая правовую основу для защиты информации и информационных систем от угроз и атак. Он помогает смягчить риски, связанные с технологическим развитием и цифровыми угрозами, и способствует обеспечению надежности и безопасности информационного пространства страны.

3)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» является ключевым законодательным актом, регулирующим сферу информационной безопасности в России. Он устанавливает общие принципы и правила обращения с информацией, охраны данных, а также права и обязанности субъектов, работающих с информацией и информационными технологиями. Федеральный закон "Об информации, информационных технологиях и о защите информации" играет важную роль в обеспечении информационной безопасности в стране, создавая правовую основу и регулируя деятельность субъектов, связанную с обработкой и защитой информации и информационных технологий. Он способствует укреплению доверия к цифровому пространству и защите личных данных граждан.

4)Закон РФ «О государственной тайне» от 21.07.1993

Закон РФ «О государственной тайне» от 21.07.1993 регулирует вопросы, связанные с определением, обладанием, использованием и раскрытием сведений, составляющих государственную тайну. С точки зрения информационной безопасности, данный закон определяет меры по защите секретной информации и обеспечению конфиденциальности данных от несанкционированного доступа. Закон "О государственной тайне" также устанавливает механизмы контроля за соблюдением требований по защите информации и проведением проверок на предмет соблюдения законодательства в сфере государственной тайны. Он обеспечивает сохранность важной информации и недопущение утечек данных, что имеет важное значение для национальной безопасности и суверенитета страны.

Федеральный закон «О коммерческой тайне» от 29.07.2004 Федеральный закон «О коммерческой тайне» от 29.07.2004 года регулирует отношения, связанные с коммерческой тайной предприятий и организаций. Этот закон важен для обеспечения информационной безопасности предприятий, так как определяет права и обязанности по охране конфиденциальной информации, которая может быть использована в коммерческих целях. Федеральный закон "О коммерческой тайне" является ключевым законодательным актом, обеспечивающим правовую защиту конфиденциальной информации предприятий и организаций, и способствующим обеспечению информационной безопасности в сфере коммерческой деятельности. Его соблюдение позволяет предотвратить несанкционированный доступ к важным коммерческим данным и сохранить конкурентные преимущества компаний.

6) Федеральный закон «О персональных данных» от 27.07.2006 Федеральный закон «О персональных данных» от 27.07.2006 года является одним из основных нормативных актов, регулирующих обработку и защиту персональных данных в Российской Федерации. С точки зрения информационной безопасности, данный закон имеет большое значение, так как он определяет правила работы с конфиденциальной информацией о частных лицах, обеспечивая их права и интересы.

Основные характеристики данного закона с точки зрения информационной безопасности:

1. Установление понятия персональных данных и их особенностей, включая информацию, относящуюся к определенному или определимому физическому лицу.

2. Установление требований к обработке персональных данных, включая сбор, хранение, использование и распространение такой информации.

3. Определение прав граждан на защиту своих персональных данных и обязанностей субъектов персональных данных (организаций и предпринимателей) по обеспечению конфиденциальности этих данных.

7) Федеральный закон «Об электронной подписи» от 06.04.2011 Федеральный закон «Об электронной подписи» от 06.04.2011 является важным нормативным актом, регулирующим вопросы использования электронной подписи в электронных документах. С точки зрения информационной безопасности, данный закон имеет большое значение, так как он определяет правила использования и признания электронных подписей, обеспечивая защиту целостности и аутентичности электронных документов. Основные характеристики данного закона с точки зрения информационной безопасности:

1. Установление понятия электронной подписи и ее роли в обеспечении безопасности электронных документов, а также определение основных принципов использования электронной подписи.

2. Установление требований к созданию и проверке электронной подписи, включая использование сертификатов ключей электронной подписи для подтверждения подлинности подписи.

8) «Уголовный кодекс Российской Федерации» от 13.06.1996 "Уголовный кодекс Российской Федерации" от 13.06.1996 года является основным нормативным актом, определяющим уголовно-правовые нормы и наказания за совершение преступлений в Российской Федерации. С точки зрения информационной безопасности, данный кодекс также имеет важное значение, так как в нем закреплены нормы, касающиеся преступлений в сфере информационных технологий и защиты информации. Основные характеристики данного кодекса с точки зрения информационной безопасности:

1. Определение уголовной ответственности за преступления, связанные с нарушением информационной безопасности, такие как незаконный доступ к компьютерной информации, создание и использование вредоносных программ, кибермошенничество и др.

2. Установление наказаний за совершение преступлений, связанных с нарушением конфиденциальности и целостности информации, включая штрафы, лишение свободы и уголовные преследования.

«Трудовой кодекс Российской Федерации» от 30.12.2001 «Трудовой кодекс Российской Федерации» от 30.12.2001 года является основным нормативным актом, регулирующим трудовые отношения между работниками и работодателями в Российской Федерации. С точки зрения информационной безопасности, данный кодекс также имеет значение, так как содержит нормы относительно защиты информации о работниках, конфиденциальности и правилах использования информации на предприятии. Основные характеристики данного кодекса с точки зрения информационной безопасности:

1. Определение прав и обязанностей работодателя и работника по обеспечению конфиденциальности информации, касающейся трудовых отношений, личных данных работников, финансовой и коммерческой информации о предприятии.

2. Установление требований к защите информации, содержащейся в трудовых документах, учетных системах и других документах, связанных с трудовыми отношениями.

10) Кодекс РФ об административных правонарушениях

"Кодекс Российской Федерации об административных правонарушениях" регулирует административную ответственность и наказание за совершение административных правонарушений. Он устанавливает меры ответственности за различные административные нарушения, включая те, которые могут относиться к области информационной безопасности. Основные характеристики данного кодекса с точки зрения информационной безопасности:

1. Определение административной ответственности за нарушения в сфере информационной безопасности, такие как незаконное получение и распространение информации, нарушение правил обработки данных, нарушение принципов защиты конфиденциальной информации и др.

2. Установление административных наказаний за нарушения законодательства в области информационной безопасности, включая штрафы, административное вынесение предупреждения, приостановление деятельности и др.

11) 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 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" является правовым актом, направленным на обеспечение информационной безопасности Российской Федерации при использовании международных информационно-телекоммуникационных сетей. Основные характеристики данного указа с точки зрения информационной безопасности:

1. Указывает на важность обеспечения информационной безопасности Российской Федерации при использовании международных информационно-телекоммуникационных сетей, учитывая современные вызовы и угрозы в области кибербезопасности.

2. Устанавливает конкретные меры и требования к обеспечению информационной безопасности при использовании международных информационно-телекоммуникационных сетей, например, в части защиты от кибератак, утечек информации, несанкционированного доступа и других угроз.

**Основные положения**

• Охрана государственной тайны и коммерческой тайны:

Законы об обеспечении конфиденциальности информации.

• Обработка персональных данных:

Нормы по обработке и защите персональных данных граждан.

• Нормы противодействия преступлениям в сфере информационных технологий:

Установление ответственности за противоправные действия и атаки на информационные системы.

• Требования к информационной безопасности:

Установление стандартов и мер по обеспечению безопасности информации и информационных систем.

**Контрольные вопросы**

1. Законодательные меры в области информационной безопасности необходимы для обеспечения защиты информации от утечек, несанкционированного доступа, уничтожения или искажения. Они помогают предотвратить нарушения конфиденциальности данных, обеспечить конфиденциальность коммерческой информации, защитить права граждан на конфиденциальность персональных данных и обеспечить безопасность критической информационной инфраструктуры.

2. Информационная безопасность в Российской Федерации регулируется рядом нормативно-правовых документов, включая:

- Федеральный закон "О безопасности" № 202-ФЗ;

- Федеральный закон "Об информации, информационных технологиях и о защите информации" № 152-ФЗ;

- Постановление Правительства Российской Федерации "Об утверждении Положения об обеспечении защиты персональных данных" № 687.

3. Основополагающие документы в области информационной безопасности в России:

- Концепция информационной безопасности Российской Федерации;

- Государственная доктрина информационной безопасности Российской Федерации;

- Стратегия национальной безопасности Российской Федерации;

- Федеральная программа "Информационное общество (2017-2030 годы)".

Эти документы определяют стратегические направления развития информационной безопасности в Российской Федерации, устанавливают принципы защиты информации и информационных ресурсов, а также определяют требования к уровню информационной безопасности в различных сферах деятельности.

Конец формы