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

Лопарев Егор

Преподаватель

Кожевников К. Д.

Казань 2024

**Часть 1**

**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.

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

Ответ: Писание на заказ вредоносных программ, даже если вы сами не используете их, наказуемо по статье 273 Уголовного кодекса и может влечь уголовную ответственность в зависимости от ущерба, причиненного действиями.

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

Ответ: Установка программы для удаленного администрирования, может рассматриваться как нарушение статьи 272 Уголовного кодекса РФ и также является уголовно наказуемым.

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

Ответ: Распространение вируса, который шифрует данные пользователей, нарушает статью 273.1 Уголовного кодекса РФ и влечет уголовную ответственность.

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

Ответ: Размещение вредоносного кода на GitHub также может попадать под статью 273.1 Уголовного кодекса РФ, потому что это распространение программы с несанкционированным доступом к информации.

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

Ответ: В случае, когда лицо моложе 18 лет совершает преступление, уголовная ответственность наступает в соответствии с Законом РФ.

f) Вы разработали код вредоносной программы, но еще

не воспользовались им.

Ответ: Разработка вредоносного программного обеспечения, даже без его использования, также может быть квалифицирована как преступление по статьям Уголовного кодекса, связанным с компьютерными преступлениями.

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

Ответ: Использование вредоносного программного обеспечения за пределами РФ не исключает возможности привлечения к уголовной ответственности в случае нарушения применимых законов о кибербезопасности.

**Контрольные вопросы**

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

2) Как правильно лицензировать программное обеспечение?

1) Административная ответственность ([Часть 1 ст. 7.12](http://base.garant.ru/12125267/4b28fea3c1f1a8d322f9fa54b177fa0f/#block_71201) КоАП РФ предусматривает ответственность за: ввоз, продажу, сдачу в прокат или иное незаконное использование экземпляров ПО в целях извлечения дохода.)

Уголовная ответственность (Уголовная ответственность за незаконное использование ПО предусмотрена [ст.146](http://base.garant.ru/10108000/0c5956aa76cdf561e1333b201c6d337d/#block_146), [272](http://base.garant.ru/10108000/8258b99e15c780ec0d7c9a628d13c3b2/#block_272), [273](http://base.garant.ru/10108000/6c61e286c98a931f79b98c1776b54fd1/#block_273) УК РФ.)

Гражданско-правовая ответственность (гражданско-правовая ответственность за нарушение интеллектуальных прав предусмотрена [ст.ст.1250 - 1253](http://base.garant.ru/10164072/22e2715446c5987f94b25b08bed9322a/#block_41250) ГК РФ.)

2) Лицензирование программного обеспечения - это процесс установления правил и условий, по которым пользователи могут использовать программное обеспечение.

1. Выбор типа лицензии: Существует несколько типов лицензий, таких как проприетарная, свободная и открытая лицензии.

2.Написание лицензионного соглашения: Создайте правила использования вашего программного обеспечения. Укажите условия, ограничения и права, которые предоставляются пользователям.

3. Распространение лицензии: Убедитесь, что лицензионное соглашение доступно для пользователей до того, как они начнут использовать ваше программное обеспечение.

**Часть №2**

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

**Задание на лабораторную работу**

1) Охарактеризовать данные документы с точки зрения информационной безопасности.

2) Выделить основные положения, которые относятся к информационной безопасности.

1)

**1. Конституция Российской Федерации:** Определяет основные принципы государственного устройства и права граждан, включая защиту информации и конфиденциальности.

2. Федеральный закон от 28.12.2010 № 390-ΦЗ «О безопасности» устанавливает правовые основы обеспечения безопасности в различных сферах деятельности, включая информационную безопасность. Закон определяет меры по защите информации в различных сферах, включая обработку, хранение, передачу и использование информации с целью обеспечения ее конфиденциальности и целостности. Также Закон устанавливает правовые основы для борьбы с киберугрозами и киберпреступностями, включая меры по предотвращению инцидентов информационной безопасности и реагированию на них.

3. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» является одним из основных законодательных актов, регулирующих информационные отношения в Российской Федерации. Закон содержит четкое определение основных понятий, связанных с информационной безопасностью, что позволяет установить единые правила и стандарты в данной области.  
Также основное внимание уделяется вопросам защиты информации от несанкционированного доступа, изменения, уничтожения или распространения, что является основным аспектом информационной безопасности. Еще устанавливаются меры ответственности за нарушения закона в области информационной безопасности, включая штрафы и иные виды наказания.

4. Закон РФ «О государственной тайне» от 21.07.1993 года является ключевым нормативным актом, регулирующим вопросы государственной тайны в России. С точки зрения информационной безопасности, этот закон имеет особое значение. Закон четко определяет, что относится к государственной тайне, а именно информация, составляющая государственную тайну и являющаяся сведениями, составляющими государственную, военную, экономическую, иные тайны.Также устанавливаются процедуры и правила доступа к информации, содержащей государственную тайну, что напрямую влияет на обеспечение ее конфиденциальности и защиту от незаконного раскрытия.

5. Федеральный закон «О коммерческой тайне» от 29.07.2004 года играет важную роль в регулировании вопросов, связанных с коммерческой тайной и ее защитой. Закон определяет, что считается коммерческой тайной, т.е., информацией о предпринимательской деятельности, которая имеет фактическое или потенциальное коммерческое значение и обладает конфиденциальным характером. Закон устанавливает правила доступа к информации, содержащей коммерческую тайну, и определяет процедуры и меры по ее защите от несанкционированного использования или раскрытия.  
Не мало важно то, что закон предписывает организациям и предпринимателям принимать меры по обеспечению конфиденциальности коммерческой информации.

6. Федеральный закон «О персональных данных» от 27.07.2006 года является ключевым нормативным актом, регулирующим сбор, обработку и хранение персональных данных в Российской Федерации. 1 Закон определяет, что считается персональными данными, т.е., любая информация, относящаяся к определенному лицу. Закон устанавливает правила и условия обработки персональных данных, включая требования к их защите от несанкционированного доступа, изменения, распространения и уничтожения. Также определяет порядок получения согласия субъекта персональных данных на их обработку, что является важным аспектом соблюдения конфиденциальности и информационной безопасности.

7. Федеральный закон «Об электронной подписи» от 6 апреля 2011 года является важным законодательным актом, регулирующим использование электронной подписи в целях обеспечения безопасности электронных документов и транзакций. Закон определяет электронную подпись как информацию в электронной форме, присоединенную к электронному документу или другим электронным данным, которая служит для определения лица, подписавшего документ, и подтверждения подлинности информации. Электронная подпись служит для защиты от подделки документов и их изменения в электронной среде, что повышает безопасность электронных коммуникаций и сделок.

8. **«Уголовный кодекс Российской Федерации»:** Содержит нормы, касающиеся противоправных действий в области информационной безопасности и их наказания.

9. Трудовой кодекс Российской Федерации охватывает широкий спектр норм, касающихся трудовых отношений и прав работников и работодателей. Трудовой кодекс устанавливает требования к составлению и хранению приказов, договоров и другой документации, касающейся трудовых отношений. Важно соблюдать конфиденциальность информации о работниках и обеспечивать безопасность их личных данных. Кодекс защищает личные данные работников. Документы, содержащие персональные сведения о сотрудниках, должны храниться безопасно и конфиденциально в соответствии с законодательством о персональных данных.

10. Кодекс Российской Федерации об административных правонарушениях устанавливает правовые нормы и ответственность за нарушения в различных сферах. Важным документом являются протоколы об административных правонарушениях, которые должны содержать достоверную информацию о нарушении и лицах, совершивших его. Безопасность протоколов включает защиту от подделки и несанкционированного доступа. Текущие документы и материалы дела по административным правонарушениям должны храниться с соблюдением конфиденциальности и безопасности информации о лицах, событиях и решениях. При обработке информации о физических лицах, в том числе в деле об административном правонарушении, необходимо соблюдать требования законодательства о персональных данных для обеспечения их конфиденциальности и защиты.

11. **Указ Президента РФ о мерах по обеспечению информационной безопасности:** Определяет меры по защите информационной безопасности при использовании информационно-телекоммуникационных сетей.

2)

* **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) 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?

1) Законодательные меры в области ИБ нужны для:

- **Защиты конфиденциальной информации:** Обеспечение безопасности и неразглашения чувствительных данных.

- **Предотвращения кибератак и нарушений безопасности:** Установление правил и ответственности для защиты информации от вредоносных действий. **- Регулирования сбора и обработки персональных данных:** Ограничение и контроль за использованием персональной информации граждан.

- **Обеспечения надежности информационных систем:** Гарантия стабильности и защиты информационных технологий.

2) В Российской Федерации информационная безопасность регулируется следующими основными документами:

**- Конституция Российской Федерации:** Включает положения о защите информации и конфиденциальности.

**- Федеральные законы:** Например, Федеральный закон «О безопасности», «Об информации, информационных технологиях и о защите информации», «О персональных данных» и т.д.

**- Постановления и указы Президента РФ.**

3) Некоторые из основополагающих документов в области информационной безопасности в Российской Федерации включают:

- **Конституция Российской Федерации:** Как основной закон страны, определяющий общие принципы защиты информации и прав граждан.

**- Федеральный закон «О персональных данных»:** Регулирует сбор, хранение и обработку информации о гражданах.

**- Федеральный закон «Об электронной подписи»:** Устанавливает правила использования электронных подписей в целях обеспечения доверия к электронным документам.