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

Иванова Я.Д.

Преподаватель

Кожевников К. Д.

Казань 2024

**Часть №1**

**Цель:**

Обосновать применение норм правового наказания при использовании ВПО.

**Ход работы:**

Для анализа данных ситуаций и определения ответственности в каждом случае по уголовному законодательству Российской Федерации, рассмотрим следующие ситуации:

a) Письменный заказ вредоносного программного обеспечения:

- Согласно статье 273.1 УК РФ, создание и распространение вредоносного программного обеспечения запрещено и влечет уголовную ответственность. В данной ситуации лицо, заказывающее создание такого программного обеспечения, может быть привлечено еще и к уголовной ответственности за статью 284 УК РФ "Организация преступного сообщества или участие в нем", если имеется организованная группа для создания и распространения вредоносных программ.

b) Установка программы для удаленного администрирования без разрешения:

- Действия системного администратора, устанавливающего программу для удаленного администрирования без ведома, могут рассматриваться в соответствии с статьей 273.1 УК РФ, связанной с нарушением информационной безопасности и использованием вредоносного ПО, и/или как нарушение статьи 274 УК РФ "Нарушение правил эксплуатации ЭВМ и Информационных систем".

c) Распространение вируса, шифрующего данные:

- В данном случае лицо может быть привлечено к ответственности по статье 273.1 или 273.2 УК РФ за создание, распространение вредоносного кода, приводящего к нанесению ущерба информационной безопасности и нарушением функционирования информационных систем и программ.

d) Размещение вируса на GitHub:

- Подобные действия также могут подпадать под статью 273 или 273.1 УК РФ, в зависимости от последствий распространения вредоносного программного обеспечения и его использования другими лицами.

e) Распространение вредоносного программного обеспечения ради интереса:

- В случае несовершеннолетнего лица, распространение вредоносного ПО ради интереса может повлечь за собой юридическую ответственность в соответствии с уголовным законодательством РФ, предусматривающему меры по возмещению ущерба и педагогическому воздействию.

f) Разработка вредоносного ПО, но не использование:

- Разработка вредоносного кода также может подпадать под статью 273.1 УК РФ, связанную с созданием и распространением вредоносного программного обеспечения.

g) Использование вредоносного ПО за пределами РФ:

- В случае, когда гражданин Российской Федерации использует вредоносное программное обеспечение за пределами страны, уголовная ответственность в основном не распространяется на такие действия согласно действующему уголовному законодательству России. Однако, следует учитывать, что в зависимости от конкретных обстоятельств и последствий таких действий, возможно привлечение к ответственности в соответствии с законодательством той страны, где фактически используется вредоносное ПО.

**Контрольные вопросы:**

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

Использование нелицензионного программного обеспечения может повлечь за собой различные виды юридической и финансовой ответственности, включая:

- Нарушение авторских прав и интеллектуальной собственности, что влечет за собой штрафы и возможные судебные разбирательства.

- Риск получения предписаний о прекращении использования нелегального ПО и уплате компенсаций.

- Ущерб бизнесу из-за возможных сбоев в работе программы, отсутствия технической поддержки, уязвимостей без обновлений и доступа к новым функциям.

1. Как правильно лицензировать программное обеспечение?

Для правильной лицензировки программного обеспечения необходимо следовать следующим принципам:

- Приобретение лицензий на все используемые программы согласно количеству и спецификации использования.

- Внимательное изучение условий лицензионного соглашения, определение типа лицензии (одноразовая, постоянная, абонентская и т.д.).

- Соблюдение всех условий использования и ограничений, предусмотренных лицензионным соглашением.

- Регулярное обновление лицензий и их контроль, чтобы избежать использования нелицензионного программного обеспечения.

- Соблюдение политики лицензирования как в корпоративных организациях, так и в частном использовании для соблюдения законодательства и обеспечения безопасности и надежности программ и данных.

**Часть №2**

**Цель:**

Ознакомиться с правовой сферой в области информационной безопасности.

**Ход работы:**

Ознакомление с перечисленными документами представляет собой важную часть в понимании законодательства Российской Федерации в области информационной безопасности. Давайте рассмотрим каждый из них и охарактеризуем с точки зрения информационной безопасности, выделим основные положения и дадим мнение по каждому документу:

a) Конституция Российской Федерации:

- Конституция устанавливает основные принципы и права граждан, в том числе их право на информационную безопасность. Она определяет общие принципы обеспечения прав и свобод граждан в информационной сфере.

b) Федеральный закон "О безопасности":

- Данный закон регулирует обеспечение безопасности деятельности в различных областях, включая информационную безопасность. Он определяет меры по предотвращению и борьбе с угрозами в информационной сфере.

c) Федеральный закон "Об информации, информационных технологиях и о защите информации":

- Регулирует использование информационных технологий, обработку и защиту информации, а также устанавливает правила для обеспечения безопасности информации.

d) Закон РФ "О государственной тайне":

- Регламентирует порядок установления, использования и охраны сведений, отнесенных к государственной тайне, в том числе в контексте информационной безопасности.

e) Федеральный закон "О коммерческой тайне":

- Устанавливает правовые основы для защиты коммерческой тайны, предполагая обеспечение конфиденциальности информации и ее безопасность.

f) Федеральный закон "О персональных данных":

- Определяет правила сбора, хранения и использования персональных данных граждан, а также меры по обеспечению их безопасности.

g) Федеральный закон "Об электронной подписи":

- Регулирует использование электронной подписи для обеспечения целостности и конфиденциальности информации, в том числе в целях информационной безопасности.

h) "Уголовный кодекс Российской Федерации":

- В содержании УК РФ существуют статьи, непосредственно связанные с нарушениями информационной безопасности, такие как статьи о компьютерных преступлениях и нарушениях в области обработки информации.

i) "Трудовой кодекс Российской Федерации":

- Устанавливает правила трудовых отношений, в том числе в части обеспечения безопасности информации и ответственности работников за разглашение конфиденциальных данных.

j) Кодекс РФ об административных правонарушениях:

- Содержит нормы, предусматривающие административную ответственность за нарушения в области информационной безопасности.

k) Указ Президента РФ "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена":

- Регламентирует меры по защите и обеспечению информационной безопасности при использовании международных информационно-телекоммуникационных сетей.

В целом, данные документы охватывают широкий спектр вопросов, связанных с информационной безопасностью, и определяют основные принципы, правила и меры для обеспечения безопасности информации. Их применение на практике способствует укреплению защиты информационных ресурсов и предотвращению угроз в информационной сфере, что является ключевым аспектом в современном цифровом мире.

**Контрольные вопросы:**

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

Законодательные меры в области информационной безопасности необходимы для обеспечения защиты информации, сохранения конфиденциальности данных, предотвращения киберугроз, борьбы с киберпреступностью, и обеспечения безопасности информационных систем в целом. Они также помогают регулировать доступ к информации, устанавливать ответственность за нарушения информационной безопасности, и обеспечивать правовую защиту владельцев информации.

2. Какими документами регулируется информационная безопасность в Российской Федерации?

В Российской Федерации информационная безопасность регулируется рядом законов и нормативных актов. Некоторыми из ключевых документов, регулирующих информационную безопасность в России, являются:

- Федеральный закон "О защите информации" от 27.07.2006 № 149-ФЗ

- Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ

- Стратегия информационной безопасности Российской Федерации на период до 2030 года

- Концепция обеспечения информационной безопасности Российской Федерации

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

Основополагающие документы в области информационной безопасности, помимо упомянутых выше, включают в себя ГОСТы (государственные стандарты), Приказы, Положения, и другие акты, регулирующие аспекты защиты информации и информационных технологий. Кроме того, важную роль играют нормативные документы ФСТЭК (Федеральной службы по техническому и экспортному контролю) и других органов, устанавливающие требования к обеспечению информационной безопасности в различных сферах деятельности.