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: «Анализ нарушений информационной безопасности»

Работу выполнил

Студент гр.4235

Вахрамеев Д.О§

Принял

Преподаватель Кожевников К.Д.

Казань 2024

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

**Часть 1**

a) Согласно Уголовному кодексу Российской Федерации, данное действие подпадает под статью 273.1 "Создание, использование и распространение вредоносных компьютерных программ" УК РФ, что влечет различные виды наказания, такие как штраф, обязательные работы и т. д.

b) Системный администратор, устанавливающий программу для удаленного администрирования RAdmin без согласия компании, может быть привлечен к уголовной ответственности в соответствии с законодательством о защите компьютерной информации или статьями УК РФ о нарушении конфиденциальности.

c) Распространение вируса, шифрующего данные на компьютерах пользователей, влечет уголовную ответственность по статье 273 "Незаконный доступ к компьютерной информации" или другим статьям, связанным с киберпреступлениями.

d) Публикация вируса на GitHub также может рассматриваться как распространение вредоносного программного обеспечения и влечет уголовную ответственность в соответствии с законодательством о кибербезопасности.

e) Независимо от возраста, распространение вредоносного программного обеспечения может повлечь уголовную ответственность согласно Уголовному кодексу.

f) Разработка вредоносной программы, даже без ее использования, также считается преступлением и может привести к уголовной ответственности.

g) Использование вредоносного программного обеспечения за пределами Российской Федерации не освобождает от ответственности перед российским законом, если такие действия противоречат законодательству РФ. В этом случае также может применяться уголовная ответственность.

Контрольные вопросы

1) Виды ответственности за использование нелегального программного обеспечения:

- Уголовная ответственность: В некоторых юрисдикциях использование нелегального программного обеспечения рассматривается как преступление, что может повлечь уголовную ответственность.

- Гражданско-правовая ответственность: Пользователи могут быть привлечены к гражданско-правовой ответственности за нарушение авторских прав при использовании нелегального программного обеспечения.

- Административная ответственность: Нарушение законодательства о лицензировании программ может привести к наложению административных штрафов со стороны регулирующих органов.

2) Процесс лицензирования программного обеспечения:

- Покупка лицензии: Для правильной лицензирования программного обеспечения следует обратиться к официальному поставщику программы или его авторизованным дистрибьюторам.

- Ознакомление с лицензионным соглашением: Важно внимательно изучить и понять условия лицензионного соглашения, чтобы соблюдать правила и ограничения использования программного обеспечения.

- Регистрация и активация: В зависимости от типа лицензии, потребуется зарегистрировать и активировать программу согласно условиям лицензионного соглашения.

- Соблюдение условий использования: После лицензирования важно соблюдать условия использования программного обеспечения, такие как количество лицензированных пользователей и обновления.

- Ведение документации: Рекомендуется вести документацию о лицензировании программного обеспечения, включая копии лицензионных ключей и договоров.

**Часть 2**

Часть 1

a) Согласно Уголовному кодексу Российской Федерации, данное действие подпадает под статью 273.1 "Создание, использование и распространение вредоносных компьютерных программ" УК РФ, что влечет различные виды наказания, такие как штраф, обязательные работы и т. д.

b) Системный администратор, устанавливающий программу для удаленного администрирования RAdmin без согласия компании, может быть привлечен к уголовной ответственности в соответствии с законодательством о защите компьютерной информации или статьями УК РФ о нарушении конфиденциальности.

c) Распространение вируса, шифрующего данные на компьютерах пользователей, влечет уголовную ответственность по статье 273 "Незаконный доступ к компьютерной информации" или другим статьям, связанным с киберпреступлениями.

d) Публикация вируса на GitHub также может рассматриваться как распространение вредоносного программного обеспечения и влечет уголовную ответственность в соответствии с законодательством о кибербезопасности.

e) Независимо от возраста, распространение вредоносного программного обеспечения может повлечь уголовную ответственность согласно Уголовному кодексу.

f) Разработка вредоносной программы, даже без ее использования, также считается преступлением и может привести к уголовной ответственности.

g) Использование вредоносного программного обеспечения за пределами Российской Федерации не освобождает от ответственности перед российским законом, если такие действия противоречат законодательству РФ. В этом случае также может применяться уголовная ответственность.

Контрольные вопросы

1) Виды ответственности за использование нелегального программного обеспечения:

- Уголовная ответственность: В некоторых юрисдикциях использование нелегального программного обеспечения рассматривается как преступление, что может повлечь уголовную ответственность.

- Гражданско-правовая ответственность: Пользователи могут быть привлечены к гражданско-правовой ответственности за нарушение авторских прав при использовании нелегального программного обеспечения.

- Административная ответственность: Нарушение законодательства о лицензировании программ может привести к наложению административных штрафов со стороны регулирующих органов.

2) Процесс лицензирования программного обеспечения:

- Покупка лицензии: Для правильной лицензирования программного обеспечения следует обратиться к официальному поставщику программы или его авторизованным дистрибьюторам.

- Ознакомление с лицензионным соглашением: Важно внимательно изучить и понять условия лицензионного соглашения, чтобы соблюдать правила и ограничения использования программного обеспечения.

- Регистрация и активация: В зависимости от типа лицензии, потребуется зарегистрировать и активировать программу согласно условиям лицензионного соглашения.

- Соблюдение условий использования: После лицензирования важно соблюдать условия использования программного обеспечения, такие как количество лицензированных пользователей и обновления.

- Ведение документации: Рекомендуется вести документацию о лицензировании программного обеспечения, включая копии лицензионных ключей и договоров.

**Вывод:** я обосновал применение норм правового наказания при использовании ВПО.