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\_

Зарифуллина М.А.

Преподаватель

Кожевников К. Д.

Казань 2024

**Часть №1**

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

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

УК РФ Статья 273. Создание, использование и распространение вредоносных компьютерных программ.

[Создание](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/), [распространение](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/) или [использование](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/) компьютерных [программ](https://www.consultant.ru/document/cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100036) либо [иной](https://www.consultant.ru/document/cons_doc_LAW_434573/7ad11c1823e584a73bbfbac49e996e617343f1ca/#dst100023) [компьютерной информации](https://www.consultant.ru/document/cons_doc_LAW_469788/5c337673c261a026c476d578035ce68a0ae86da0/#dst978), заведомо предназначенных для несанкционированного [уничтожения](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/), [блокирования](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/), [модификации](https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/), [копирования](https://www.consultant.ru/document/cons_doc_LAW_161817/2e91d385fb5ad4a0d4cf31b897557e83e5e64009/#dst100028) компьютерной информации или [нейтрализации](https://www.consultant.ru/document/cons_doc_LAW_434573/7ad11c1823e584a73bbfbac49e996e617343f1ca/#dst100016) средств защиты компьютерной информации, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

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

**Статья 361 УК РФ "Повреждение или уничтожение информации, сведений, программного обеспечения или баз данных"**: Применяется к случаям умышленного уничтожения или повреждения информации, программного обеспечения или баз данных.

УК РФ Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Нарушение [правил](https://www.consultant.ru/document/cons_doc_LAW_434573/7ad11c1823e584a73bbfbac49e996e617343f1ca/#dst100033) эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее [уничтожение](https://www.consultant.ru/document/cons_doc_LAW_10699/b5a4306016ca24a588367791e004fe4b14b0b6c9/), [блокирование](https://www.consultant.ru/document/cons_doc_LAW_10699/b5a4306016ca24a588367791e004fe4b14b0b6c9/), [модификацию](https://www.consultant.ru/document/cons_doc_LAW_10699/b5a4306016ca24a588367791e004fe4b14b0b6c9/) либо [копирование](https://www.consultant.ru/document/cons_doc_LAW_10699/b5a4306016ca24a588367791e004fe4b14b0b6c9/) [компьютерной информации](https://www.consultant.ru/document/cons_doc_LAW_469788/5c337673c261a026c476d578035ce68a0ae86da0/#dst978), причинившее [крупный ущерб](https://www.consultant.ru/document/cons_doc_LAW_469788/5c337673c261a026c476d578035ce68a0ae86da0/#dst979), -

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

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

1. Статья 273.1 УК РФ "Создание, использование и распространение вредоносных компьютерных программ". Предусматривает наказание в виде штрафа до 500 тысяч рублей или лишения свободы на срок до двух лет.

2. Статья 272 УК РФ "Незаконный доступ к компьютерной информации". Причинение значительного ущерба может повлечь более строгое наказание, включая лишение свободы на срок до пяти лет.

3. Статья 273 УК РФ "Нарушение правил эксплуатации ЭВМ и баз данных". Если ваше действие привело к нарушению работы информационной системы или базы данных, вы можете быть привлечены к уголовной ответственности.

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

Действия по выкладыванию вируса на GitHub могут быть квалифицированы по статье 273 Уголовного кодекса Российской Федерации "Незаконный доступ к компьютерной информации". Согласно этой статье, незаконный доступ к компьютерной информации, совершенный путем взлома защиты информационной системы или иным способом, наказывается штрафом до 200 тысяч рублей или арестом до шести месяцев.

**Статья 272.3 УК РФ "Нарушение правил защиты информации"**: Регулирует нарушение правил защиты информации, включая недопустимое распространение вредоносных программ.

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

**Статья 138.1 УК РФ "Незаконные действия в сфере информационных технологий"**: Данная статья устанавливает уголовную ответственность за незаконные действия в сфере информационных технологий, включая распространение вредоносных программ.

Статья 273.1 УК РФ "Создание, использование и распространение вредоносных компьютерных программ". Данная статья предусматривает наказание в виде штрафа до 300 тысяч рублей или обязательные работы на срок до 360 часов, либо исправительные работы на срок до одного года.

Статья 272 УК РФ "Незаконный доступ к компьютерной информации". Причинение значительного ущерба может повлечь более строгое наказание, включая лишение свободы на срок до трех лет.

Статья 273 УК РФ "Нарушение правил эксплуатации ЭВМ и баз данных". В случае нарушения работы информационной системы или базы данных, вы также можете быть привлечены к уголовной ответственности.

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

1. Статья 273.1 УК РФ "Создание, использование и распространение вредоносных компьютерных программ". Данная статья предусматривает наказание за создание вредоносной программы, независимо от того, была ли она использована или распространена. Вам может быть предъявлено обвинение и назначено наказание в виде штрафа до 300 тысяч рублей, обязательных работ на срок до 360 часов или исправительных работ на срок до одного года.

2. **Статья 146 УК РФ "Нарушение авторских и смежных прав"**:

Нарушение авторских прав при создании вредоносного ПО или использовании чужих программных продуктов без разрешения может подпадать под действие данной статьи.

3. **Статья 272.1 УК РФ "Нарушение правил обращения в Российской Федерации с техническими средствами защиты информации"**: Применяется к случаям нарушения правил обращения с техническими средствами защиты информации, которые могут быть связаны с разработкой вредоносного программного обеспечения.

g) Если вы, как гражданин РФ, используете вредоносное программное обеспечение исключительно за пределами Российской Федерации, то применение Уголовного кодекса РФ к вашим действиям может быть ограничено. Однако, в некоторых случаях уголовная ответственность может быть предусмотрена в соответствии с российским законодательством.

1. Статья 273.1 УК РФ "Создание, использование и распространение вредоносных компьютерных программ". По данной статье может быть возбуждено уголовное дело, если вы как гражданин РФ использовали вредоносное ПО за пределами страны. Наказание предусмотрено в виде штрафа до 300 тысяч рублей, обязательных работ на срок до 360 часов или исправительных работ на срок до одного года.

Уголовная ответственность может быть применена к действиям, совершенным гражданином РФ за пределами страны, если эти действия признаются преступными согласно законодательству РФ и, если существует международное соглашение о взаимной правовой помощи в уголовных делах между Россией и страной, где было совершено преступление.

**Контрольные вопросы**

1. Перечислите виды ответственности при использовании нелицензионного программного обеспечения.

При использовании нелицензионного программного обеспечения может возникнуть различная юридическая ответственность. Вот некоторые общие виды ответственности за использование нелицензионного ПО:  
1.) **Административная ответственность**: Нарушение авторских прав и использование нелицензионного ПО может повлечь административные штрафы и санкции со стороны государственных органов  
2.) **Гражданская ответственность**: При обнаружении использования нелицензионного ПО правообладатель имеет право на возмещение ущерба, причиненного использованием ПО без лицензии.  
3.) **Уголовная ответственность**: В случае кражи, распространения или использования взломанного программного обеспечения могут быть применены уголовные статьи, такие как статьи о нарушении авторских прав.

1. Как правильно лицензировать программное обеспечение?

Чтобы правильно лицензировать программное обеспечение нужно следовать основным пунктам:  
1. **Покупка лицензии**: Приобретение лицензии на программное обеспечение у правообладателя (через покупку или аренду).  
2. **Соблюдение условий лицензионного соглашения**: Важно внимательно читать и соблюдать условия лицензионного соглашения, включая количество лицензируемых копий, переуступку и прочие ограничения.  
3. **Регистрация и активация лицензии**: В некоторых случаях требуется регистрация и активация лицензии, чтобы обеспечить ее действительность и использование.  
4. **Обновление и поддержка**: Поддержание актуальной лицензии и обновлений для безопасности и совместимости.

**Часть №2**

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

1. Охарактеризуйте данные документы с точки зрения информационной безопасности:  
   - Конституция Российской Федерации: Основной закон, который устанавливает принципы прав и свобод человека и гражданина, обеспечивая защиту информационной безопасности граждан и государства.  
     
   - Федеральный закон "О безопасности": Направлен на обеспечение общенациональной безопасности, включая информационную безопасность государства и граждан.  
     
   - Закон РФ "О государственной тайне": Регулирует вопросы об охране сведений государственной тайны, важных для информационной безопасности России.  
     
   - Федеральный закон "О коммерческой тайне": Устанавливает меры по защите конфиденциальной информации коммерческих структур. Важно для защиты конфиденциальности и информационной безопасности предприятий.  
     
   - Федеральный закон "О персональных данных": Регулирует обработку и защиту персональных данных граждан, что крайне важно для обеспечения конфиденциальности и безопасности личной информации.  
     
   - Федеральный закон "Об электронной подписи": Устанавливает правовые основы использования электронной подписи, влияющей на безопасность электронных документов и связанных с ними процессов.  
     
   - Уголовный и Трудовой кодексы РФ: Включают нормы, касающиеся ответственности за нарушения в области информационной безопасности и прав граждан.  
     
   - Указ Президента РФ "О мерах по обеспечению информационной безопасности": Определяет меры по обеспечению безопасности информационного пространства и защите информации в сетях связи.  
     
   3. Основные положения, относящиеся к информационной безопасности:  
     
   -  Защита государственных и коммерческих тайн.  
   - Обеспечение конфиденциальности и безопасности персональных данных.  
   - Использование электронной подписи для обеспечения целостности и подлинности документов.  
   - Установление ответственности за нарушения в области информационной безопасности.  
   - Принятие мер по защите информационных ресурсов и систем от угроз и атак.  
   - Регулирование обработки и передачи информации в соответствии с законодательством.  
   - Установление профессиональных и технических стандартов обеспечения информационной безопасности.  
     
   Эти документы и законы играют важную роль в обеспечении безопасности информации, как на государственном, так и на коммерческом уровне, обеспечивая защиту данных, конфиденциальности и прав граждан.11:52

**Контрольные вопросы**

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

Законодательные меры в области информационной безопасности необходимы для: защиты конфиденциальной информации, предотвращения киберугроз и кибератак, защиты персональных данных граждан, установления правил и ответственности за нарушения в области информационной безопасности, регулирования использования электронной подписи и шифрования данных, обеспечения безопасного функционирования информационных систем и сетей.

1. Какими документами регулируется информационная    безопасность в Российской Федерации?

Конституцией Российской Федерации, Федеральным законом «О безопасности», Федеральным законом «О персональных данных», Федеральным законом «Об электронной подписи», Указами президента о мерах по обеспечению информационной безопасности.

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

Конституция РФ, Федеральный закон «О безопасности», Федеральный закон «О персональных данных».