Задания:

1. Сделать конспект темы «Ответственность в информационной сфере: Гражданско-правовая и административная ответственность в информационной сфере»
2. Сделать конспект темы «Ответственность в информационной сфере: Уголовная ответственность»
3. Сделать конспект темы «Ответственность в информационной сфере: Понятие и основные направления компьютерных преступлений, и их предупреждение»
4. Сделать конспект темы «Ответственность в информационной сфере: Правовое регулирование в информационной сфере. Проблема информационной безопасности» + тестовая работа по теме.

Тема 1.5. Ответственность в информационной сфере

Тема 1.5.1. Гражданско-правовая и административная ответственность в информационной сфере

В механизме правового обеспечения в информационной сфере значимое место занимают борьба с нарушениями информационного законодательства и их предупреждение. Для этого действует так называемый институт юридической ответственности, закрепленный в российском законодательстве.

В настоящее время сформирована основная нормативная база по предупреждению и пресечению правонарушений в информационной сфере, предусматривая как гражданско-правовая, дисциплинарная (включая материальную), административная ответственность, так и уголовная ответственность за совершение правонарушений и преступлений в информационной сфере, разработаны и действуют многочисленные законы и подзаконные акты в информационной сфере.

Юридическая ответственность реализуется с учетом специфических методов информационного права при возникновении конфликтных противоправных ситуаций. Дисциплинарная ответственность наступает за противоправные действия, совершаемые субъектами информационного права в связи с исполнением своих прав и обязанностей. Административная ответственность устанавливается за нарушение определенных правил поведения.

В Кодексе об административных правонарушениях предусматривается административная ответственность.

Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

Статья 13.12. Нарушение правил защиты информации.

Статья 13.13. Незаконная деятельность в области защиты информации.

Отсюда следует, что при административном судопроизводстве могут быть наложены следующие виды административных взысканий:

- предупреждение – мера административного наказания, выраженная в официальном порицании физического или юридического лица, выносимого в письменной форме;
- административный штраф – денежное взыскание;
- возмездное изъятие орудия совершения или предмета административного правонарушения;
- принудительное изъятие и последующая реализация с передачей бывшему собственнику вырученной суммы за вычетом расходов на реализацию;
- конфискация орудия совершения или предмета административного правонарушения;

- лишение специального права;
- административный арест;
- административное выдворение за пределы РФ иностранного гражданина или лица без гражданства;
- дисквалификация – лишение права занимать руководящие должности в исполнительных органах управления юридических лиц;
- административное приостановление деятельности.

Объектом правонарушения является совокупность общественных отношений в информационной сфере.

Информация (сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления), документированная информация, компьютерная информация могут являться предметом правонарушения в информационной сфере.

Согласно Федеральному закону «Об информации, информатизации и защите информации» юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие её, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации (ст. 11).

Статьей 15 этого же Закона определены обязанности и ответственность владельца информационных ресурсов: владелец информационных ресурсов несет юридическую ответственность за нарушение правил работы с информацией в порядке, предусмотренном законодательством Российской Федерации.

Защита прав субъектов в сфере информационных процессов и информатизации предусмотрена ст. 23 Закона: за правонарушения при работе с документированной информацией органы государственной власти, организации и их должностные лица несут ответственность в соответствии с законодательством Российской Федерации и её субъектов.

Закон об интернет-пиратстве

Со 2 июля 2013 г. вступил в силу Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях» (Федеральный закон от 21.06.2013 г. № 187-ФЗ принят Гос. Думой, одобрен Советом Федерации 26.06.2013 г., подписан Президентом РФ В. В. Путиным 02.07.2013 г., вступил в силу с 01.08.2013 г.) (Закон о борьбе с пиратством).

Тема 1.5.2. Уголовная ответственность

Уголовная ответственность в Российской Федерации определяется Уголовным Кодексом. Уголовный Кодекс Российской Федерации (УК РФ от 13.06.1996 № 63-ФЗ (ред. от 17.04.2017 г.)) является единственным нормативным документом, который устанавливает, какое действие является преступлением, какое наказание предусмотрено за совершение конкретного преступления. В Уголовном кодексе РФ к преступлениям в информационной сфере можно отнести более 50 статей, причем отдельная глава УК РФ (гл. 28) посвящена составам преступлений в сфере компьютерной информации.

Тема 1.5.2.1. Киберпреступление

Ускоренное развитие общества, его стремление к упразднению границ, интеграции и глобализации влекут за собой различные последствия, к несчастью, не всегда позитивные.

Достижения науки и техники, создание всемирной сети Интернет позволили преступности выйти на новый уровень и захватить киберпространство.

Теперь преступнику не нужен прямой контакт с жертвой и всего несколько человек могут стать угрозой для каждого пользователя «глобальной паутины», крупных корпораций и целых государств.

Киберпреступность — это преступность в так называемом виртуальном пространстве. *Виртуальное пространство, или киберпространство* можно определить как моделируемое с помощью компьютера информационное пространство, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленные в математическом, символьном или любом другом виде и находящиеся в процессе движения по локальным и глобальным компьютерным сетям, либо сведения, хранящиеся в памяти любого физического или виртуального устройства, а также другого носителя, специально предназначенного для их хранения, обработки и передачи.

С различать **киберпреступления как правовую категорию и киберпреступность как социальное явление**. Последнее включает в себя не только совокупность всех данных преступлений, но и различные формы тесно связанных с ними «поддерживающей» и организационной деятельности. В этом смысле обмен электронной почтой между лицами, готовящими преступление, размещение соответствующей криминально ориентированной информации на в web-сайтах также относятся или, во всяком случае, примыкают к киберпреступности как социальному явлению.

Киберпреступление – это любое преступление в электронной сфере, совершенное при помощи компьютерной системы или сети, или против них.

Удалось выявить и *особенности данного вида преступлений*, это:

1. чрезвычайная скрытность деяний, которая достигается применением механизмов анонимности и шифрования;
2. трансграничность, преступник и жертва могут быть разделены тысячами километров, границами нескольких государств;
3. нестандартность способов совершения;
4. автоматизированный режим.

Поскольку киберпреступления охватывают широчайший пласт общественных отношений, предполагают, использование различного оборудования и имеют целый спектр способов совершения, логично провести их классификацию.

Конвенция Совета Европы о киберпреступности говорит, о четырех типах компьютерных преступлений «в чистом виде», определяя их как преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

- Незаконный доступ — ст. 2 (противоправный умышленный доступ к компьютерной системе либо ее части);
- Незаконный перехват — ст. 3 (противоправный умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему, с нее либо в ее пределах);
- Вмешательство в данные — ст. 4 (противоправное повреждение, удаление, нарушение, изменение либо пресечение компьютерных данных);
- Вмешательство в систему — ст. 5 (серьезное противоправное препятствование функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, нарушения, изменения либо пресечения компьютерных данных).

Именно эти четыре вида преступлений являются **собственно «компьютерными»**, остальные — это либо **связанные с компьютером** (computer-related), либо **совершаемые с помощью компьютера** (computer-facilitated) преступления.

К ним относятся:

- преступлении, связанные с нарушением авторских и смежных прав;
- действия, где компьютеры используются как орудия преступления (электронные хищения, мошенничества и т.п.);
- преступления, где компьютеры играют роль интеллектуальных средств (например, размещение в сети Интернет детской порнографии, информации, разжигающей национальную, расовую, религиозную вражду и т.д.).

Количество киберпреступлений, совершаемых в России и в мире, неуклонно растет, **за последние пять лет их число колеблется в пределах 8 тыс. – 17 тыс., с ежегодной динамикой около 10%**.

Меняется и их качественный состав, и размер причиненного ущерба.

Такое торжество преступности в виртуальном пространстве не может обойтись безнаказанно.

Ответственность за киберпреступления в России предусматривается главой 28 УК РФ и касается только компьютерных преступлений.

В зависимости от тяжести преступления и размера причиненного вреда статьи 272,273 и 274 УК РФ предполагают наказание в виде штрафа от 100 тыс. рублей, исправительных или принудительных работ от 6 месяцев до 5 лет, ограничения или лишения свободы до 7 лет. Возможно сочетание видов наказания.

Тема 1.5.2.2. Понятие и основные направления компьютерных преступлений, и их предупреждение.

Компьютерные преступления – это предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства.

Компьютерные преступления условно можно подразделить на две большие категории:

1. Преступления, связанные с вмешательством в работу компьютеров;
2. Преступления, использующие компьютеры как необходимые технические средства.

Основные виды преступлений:

В 2009 году были осуждены два студента из Архангельска за размещение в социальной сети экстремистских материалов, житель Пскова за распространение порнографии, а также житель Ижевска за взлом одной из страничек.

Преступление: Размещение в социальной сети экстремистских материалов

Уголовная ответственность:

Раздел 9. Преступления против общественной безопасности и общественного порядка

Глава 24. Преступления против общественной безопасности

Статья 205.2. Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма

Раздел 10. Преступления против государственной власти

Глава 29. Преступления против основ конституционного строя и безопасности государства

Статья 280. Публичные призывы к осуществлению экстремистской деятельности

Статья 282. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства

Преступление: Распространение порнографии

Уголовная ответственность:

Статья 242. Незаконное распространение порнографических материалов или предметов

Статья 242.1. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (введена Федеральным законом от 08.12.2003 N 162-ФЗ)

Преступление: Взлом странички в социальной сети

Уголовная ответственность:

1) 138 статья Уголовного Кодекса РФ. Предусматривает штраф до 80 000 рублей или исправительные работы сроком до года или обязательные работы сроком до 360 часов. В данном случае, речь идет о нарушении тайн переписок, почтовых и электронных сообщений, телефонных переговоров.

2) 272 статья Уголовного Кодекса РФ. Здесь предусмотрен более серьезный штраф (до 200 000 рублей) либо исправительные работы до 1 года либо лишение свободы сроком до 2 лет.

Таким образом, взлом страницы вконтакте — совсем не баловство, а серьезное уголовное преступление, за него можно получить реальный срок.

В январе 2011 года против одного из пользователей «ВКонтакте» было возбуждено уголовное дело по обвинению в нарушении авторских прав.

Преступление: Нарушение авторских прав

Уголовная ответственность:

УК РФ Статья 146. Нарушение авторских и смежных прав

---

28 февраля 2011 года пользователю «ВКонтакте» Александру Домрачёву были предъявлены обвинения в «пропаганде ненависти и вражды к определённой социальной группе» — так следствие расценило размещённый пользователем призыв «Бей ментов, спасай Россию» в одной из групп «ВКонтакте». Поводом для привлечения Домрачева к уголовной ответственности также послужила сама созданная им группа, а именно — за размещённые там оскорбительные фотографии и комментарии в адрес сотрудников полиции.

Преступление: Пропаганда ненависти и вражды к определенной социальной группе

Уголовная ответственность:

Статья 282 УК РФ. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства

Хакерство – это несанкционированное вмешательство в программное обеспечение с целью изменения первоначальных функций и достижения целей, непредусмотренных первоначально создателем.

Хакер, «компьютерный пират» - лицо, совершающее несанкционированные доступы в компьютерные системы с целью развлечения, нанесения ущерба (в том числе и путем распространения компьютерных вирусов).

Хакер – это чрезвычайно квалифицированный специалист, «компьютерный взломщик», который последовательностью действий перехватывает информацию, копирует полученные данные для последующего использования её в преступных целях, таких как вымогательство денежных средств или банковское мошенничество.

В российских законах недавно появилась статья предусматривающая наказание за разработку и распространение компьютерных вирусов.

Уголовная ответственность:

Статья 272. Неправомерный доступ к компьютерной информации

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

Компьютерное мошенничество – это преступная деятельность, связанная с завладением чужим имуществом путем обмана или злоупотребления доверием, совершеннее при помощи средств компьютерной техники.

Различают следующие виды компьютерного мошенничества:

- распространение противозаконных материалов и содействие бизнесу, основанному на мошенничестве;
- различные информационные службы активно используют доверие граждан для получения денежных средств, пропагандируя быстрые способы обогащения и чудесное похудение.

Уголовная ответственность:

Статья 159.6. Мошенничество в сфере компьютерной информации

Тема 1.5.3. Правовое регулирование в информационной сфере. Проблема информационной безопасности

За последние годы в Российской Федерации реализован комплекс мер по совершенствованию обеспечения ее информационной безопасности. Начато формирование базы правового обеспечения информационной безопасности.

Приняты Закон Российской Федерации "О государственной тайне", Основы законодательства Российской Федерации об Архивном фонде Российской Федерации

и архивах, федеральные законы "Об информации, информатизации и защите информации", "Об участии в международном информационном обмене", ряд других законов, развернута работа по созданию механизмов их реализации, подготовке законопроектов, регламентирующих общественные отношения в информационной сфере.

Осуществлены мероприятия по обеспечению информационной безопасности в федеральных органах государственной власти, органах государственной власти субъектов Российской Федерации, на предприятиях, в учреждениях и организациях независимо от формы собственности. Развернуты работы по созданию защищенной информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти.

Успешному решению вопросов обеспечения информационной безопасности Российской Федерации способствуют государственная система защиты информации, система защиты государственной тайны, системы лицензирования деятельности в области защиты государственной тайны и системы сертификации средств защиты информации.

Вместе с тем анализ состояния информационной безопасности Российской Федерации показывает, что ее уровень не в полной мере соответствует потребностям общества и государства.

Некоторые законы, действующие в информационной сфере в Российской Федерации.

1. ФЗ РФ №149-ФЗ «Об информации, информационных технологиях и о защите информации», принят Государственной думой 8 июля 2006 года, одобрен Советом Федерации 14 июля 2006 года. http://www.rg.ru/2006/07/29/informacia-dok.html
2. Закон РФ "О правовой охране программ для ЭВМ и баз данных", подписан Президентом Российской Федерации Б.Ельциным, 23 сентября 1992 года N 3523-1 http://lemoi-www.dvgu.ru/unir/ois/ois_zakon_o_prav_ohrane_pc&bd.htm
3. Преступления в сфере компьютерной информации. Уголовный кодекс РФ. http://www.base.garant.ru/10108000/29/
4. ФЗ РФ №152-ФЗ «О персональных данных», принят Государственной думой 8 июля 2006 года, одобрен Советом Федерации 14 июля 2006 года. http://www.rg.ru/2006/07/29/personaljnye-dannye-dok.html.

Необеспеченность прав граждан на доступ к информации, манипулирование информацией вызывают негативную реакцию населения, что в ряде случаев ведет к дестабилизации социально-политической обстановки в обществе.

Решение задач из практикума с.19-20. (газета «Информатика», №4, 2010, приложение к газета «Первое сентября»):

1. Небольшая компьютерная фирма занималась продажей компьютеров с предустановленной нелицензионной версией операционной системы Windows XP. Она имеет легально закупленную ранее у компании — представителя фирмы Microsoft лицензионную версию Windows-2000, которая устанавливалась ранее на продаваемые компьютеры. Является ли установка Windows XP нарушением лицензионных прав и почему?
2. Сотрудник экологической службы военного завода из экологических побуждений передал корреспонденту газеты правдивую информацию о состоянии загрязнения на заводе. Газета из соображений реализации тиража преподнесла эту информацию в отягощенном виде. Нарушено ли здесь информационное право? Опишите сценарий разбирательства.
3. В служебные обязанности сетевого администратора фирмы входит ежедневный антивирусный контроль. Из-за спешки он однажды не сделал этого, в результате чего вирус уничтожил важные данные. Администратором и другими сотрудниками фирмы было потеряно достаточно большое время и большие ресурсы для восстановления утерянных данных. Руководство фирмы решило вычесть из зарплаты сетевого администратора все понесенные затраты. Право ли руководство фирмы и почему? Опишите сценарий разбирательства.
4. Некто разместил копии фотографий из публичного журнала с широко известной торговой маркой на своем интернет-сайте. Нарушил ли он Закон об авторском праве и почему? Опишите сценарий разбирательства.

Закрепленные в Конституции Российской Федерации права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки практически не имеют достаточного правового, организационного и технического обеспечения. Неудовлетворительно организована защита собираемых федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления данных о физических лицах (персональных данных).

Знакомство с кратким изложением модуля «Безопасность и конфиденциальность при работе с компьютером» программы дистанционного курса «Твой курс». Можно заниматься в интерактивном и автономном режимах. (Программа «Основы компьютерной грамотности») http://ycdl.ph-int.org/study/4/. – 15 мин.

Разобрать пример.

Николай Новиков работает в редакции газеты. Ему нужно написать статью о компьютерных технологиях. Николай копирует часть информации с одного из веб-сайтов и использует ее в своей статье. Однако он не ссылается на источник, откуда взята данная информация. После публикации статьи Николай сталкивается с

юридическими проблемами из-за нарушения авторского права. Это связано с тем, что он использовал интеллектуальную собственность без разрешения владельца.

Любая доступная в Интернете информация является интеллектуальной собственностью, которая по закону принадлежит создавшему ее лицу. Например, если Вы опубликовали на веб-сайте статью, данная статья является вашей интеллектуальной собственностью. Как владелец интеллектуальной собственности, Вы обладаете эксклюзивными правами на следующие виды деятельности:

- Копирование, воспроизведение или распространение собственности.
- Совместное использование прав на собственность или их продажа.
- Бесплатная передача прав на собственность.

Примечание

Фактические права на интеллектуальную собственность могут варьироваться в зависимости от разрешений, полученных от владельца.

Использование интеллектуальной собственности без разрешения владельца запрещено. Существуют законы, защищающие права людей на интеллектуальную собственность. Такие законы называются законами *об авторском праве*. Нарушение таких законов может вызвать юридические проблемы.

Юридические вопросы, связанные с использованием материалов, охраняемых авторским правом.

На веб-сайте Вы можете получить разрешение на загрузку охраняемой авторским правом информации. Однако при загрузке такой информации Вы можете столкнуться с юридическими последствиями. Как правило, размещенная на веб-сайте информация официально охраняется авторским правом и сопровождается уведомлением об авторском праве или помечена специальным знаком. Однако отсутствие такого уведомления или знака еще не означает, что информация не охраняется авторским правом. Согласно законодательству об авторском праве Великобритании, как только человек облек идею или концепцию в физическую форму, работа автоматически становится материалом данного лица, который охраняется авторским правом. Таким же образом, согласно законодательству об авторском праве США, владелец авторского права обладает эксклюзивными правами на материалы, охраняемые авторским правом, даже без официальной регистрации авторского права.

Нарушение авторского права в любой форме является наказуемым правонарушением. Владелец авторского права может подать судебный иск против лица, нарушившего закон об авторском праве, или может потребовать крупную компенсацию за такое нарушение. Поэтому, прежде чем загружать какую-либо

информацию с веб-сайта, ознакомьтесь с международным и местным законодательством об авторском праве.

Легальное использование материалов, охраняемых авторским правом.

В следующей таблице приведены примеры легального использования материалов, охраняемых авторским правом.

Легальное использование	**Описание**
Использование охраняемых авторским правом материалов в обучающих целях	Использование Вами небольших объемов охраняемых авторским правом материалов в обучающих целях с указанием источника является добросовестным использованием таких материалов. Например, в школьном или университетском задании Вы можете использовать материалы из книги в небольшом объеме с указанием названия данной книги. Аналогично, если Вы пишете рецензию на книгу, Вы можете цитировать отрывки из данной книги.
Использование ссылок вместо использования загруженных материалов	Вместо того чтобы копировать материалы с веб-сайтов и использовать их в своей работе, можно привести ссылки на данные материалы. Например, Вы хотите упомянуть в своей статье материалы, опубликованные на определенном веб-сайте. Вместо того, чтобы копировать данные материалы с веб-сайта, просто приведите ссылку на данный веб-сайт в своей статье. Таким образом Вы полностью избежите плагиата материалов, охраняемых авторским правом.
Использование охраняемых авторским правом материалов с разрешения владельца	Вы можете использовать охраняемые авторским правом материалы в своей работе, получив на это разрешение от владельца авторских прав. В большинстве случаев для использования таких материалов требуется письменное разрешение. Помните о том, что владелец авторских прав может на свое усмотрение: • Выдать разрешение на использование охраняемых авторским правом материалов или отказать в выдаче такого разрешения. • Дать право на использование какой-либо части охраняемого авторским правом материала или

	всего материала. • Брать оплату за выдачу разрешения на использование охраняемых авторским правом материалов. • Определять условия использования охраняемых авторским правом материалов. Например, Вам может быть разрешено загрузить охраняемое авторским правом программное обеспечение и передавать его другим пользователям, но не разрешено использовать его для извлечения прибыли. Если срок действия авторского права на материалы истек либо идея или процесс, используемые в охраняемых авторским правом материалах, стали общеизвестными, данные материалы или идею можно использовать без получения разрешения.

Ответить на вопросы:

1. Ответственность по УК РФ наступает при:

1) рекламе лекарства;
2) клевете;
3) описании событий произошедшего террора;
4) описании медицинских показаний нарковещества

2. Если по электронной почте пришел спам, то лучше всего:

1) сохранить его на жестком диске в виде архива;
2) прочитать все тексты и приложения и удалить ненужное;
3) записать адрес источника и выяснить затем его IP-адрес;
4) удалить все, не читая.

3. Компьютерный вирус обычно срабатывает:

1) при очень большом числе обращений к серверу;
2) во время отсутствия пользователя;
3) используя IP-адрес компьютера;
4) перехватывая управление от работающей программы.

4. АРМ — это система:

1) автоматического ведения работ профессионала;
2) автоматизированного ведения работ профессионала;
3) автоматизации работы менеджера;

4) автоматического составления расписания работ.

5. Отличительная сторона информационного общества:

1) информационная конфиденциальность;
2) массовое производство компьютеров во всех странах;
3) информационная открытость;
4) организация конференций и диспутов.

6. Глобализация подразумевает унификацию:

1) политического строя;
2) национальных экономик;
3) социального положения;
4) медицинских систем.

7. "Электронное правительство" — это:

1) инфраструктура;
2) кабинет министров;
3) интернет-сообщество;
4) проект.

8. Наиболее типично нарушение в Интернете в области:

1) административного права;
2) прав интеллектуальной собственности;
3) уголовного права;
4) гражданского права.

9. Наиболее распространенными являются следующие классы угроз:

1) ошибки эксплуатации и изменения режима работы системы;
2) непреднамеренные действия;
3) продажа нелицензионного программного обеспечения;
4) использование старой техники.

10. Основная цель концепции государственной информационной политики РФ:

1) информационное образование населения;
2) определение целей, задач и объектов этой политики;
3) обеспечение информационной безопасности РФ;
4) вхождение в информационное мировое сообщество.