**МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ имени И.Т. ТРУБИЛИНА»**

Юридический факультет

Кафедра криминалистики

**ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ**

**Методические указания**

для организации контактной работы собучающимися по

направлению подготовки 40.04.01 Юриспруденция

Краснодар

КубГАУ

2021

*Составители:*В. В. Помазанов, С. И. Грицаев.

**Информационно-коммуникационные технологии и информационная безопасность в юридической деятельности:** метод. указания / сост. В. В. Помазанов, С. И. Грицаев. – Электронный ресурс, 2021. – 22 с.

Методические указания содержат краткую характеристику основных аспектов контактной работы (аудиторной и внеаудиторной) преподавателя с обучающимися при изучении дисциплины «Информационно-коммуникационные технологии и информационная безопасность в юридической деятельности», требования по ее выполнению.

Предназначены для обучающихся по направлению подготовки 40.04.01 Юриспруденция.

© В. В. Помазанов,

 С. И. Грицаев

составление, 2021

© ФГБОУ ВО «Кубанский

государственный аграрный
университет имени
И. Т. Трубилина», 2021

**ВВЕДЕНИЕ**

Цель организации контактной работы преподавателя с обучающимся по дисциплине «Информационно-коммуникационные технологии и информационная безопасность в юридической деятельности» – обеспечение качества общекультурной и профессиональной подготовки обучающихся по направлению подготовки 40.04.01 Юриспруденция, что позволяет выпускнику успешно работать в избранной сфере деятельности, обладать компетенциями, способствующими его социальной мобильности и конкурентоспособности в современных условиях.

Контактная работа преподавателя с обучающимся по дисциплине «Информационно-коммуникационные технологии и информационная безопасность в юридической деятельности» может быть аудиторной и внеаудиторной. Объем контактной работы отражается в учебных планах.

Контактная работа преподавателя с обучающимся по дисциплине «Информационно-коммуникационные технологии и информационная безопасность в юридической деятельности» включает в себя: занятия лекционного типа, семинары, практические, индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации и проведение зачета.

Качество освоения обучающимся материала по дисциплине «Информационно-коммуникационные технологии и информационная безопасность в юридической деятельности» оценивается преподавателем в ходе контактной работы (аудиторная и внеаудиторная) с обучающимся посредством текущего контроля успеваемости и промежуточной аттестации обучающихся (период сдачи зачета).

Текущий контроль, осуществляемый преподавателем, обеспечивает выполнение обучающимся всех видов работ, предусмотренных рабочей программой дисциплины (устный опрос, решение компетентностно-ориентированных задач (ситуационных), участие в дискуссиях, тестирование)*,* активность обучающегося в ходе учебной деятельности, посещаемость занятий, научно-исследовательскую работу и т.д.

Формой промежуточной аттестации обучающихся по дисциплине «Информационно-коммуникационные технологии и информационная безопасность в юридической деятельности» является зачет.

**1. АУДИТОРНАЯ КОНТАКТНАЯ РАБОТА ПРЕПОДАВАТЕЛЯ С ОБУЧАЮЩИМИСЯ ПО ДИСЦИПЛИН «Информационно-коммуникационные технологии и информационная безопасность в юридической деятельности»**

1.1 ПЛАНЫ ПРАКТИЧЕСКИХ (СЕМИНАРСКИХ)

ЗАНЯТИЙ

# Тема 1. Информационное общество и информатизация

**План занятия:**

1. Информация и данные.

2. Виды информации.

3. Системы связи и обмена информацией.

**Задания:**

**1. Доклад**

Тема доклада:

Право и информационные технологии.

**2. Реферат**

Тема реферата:

Государственная политика в сфере использования информационных технологий в органах государственной власти.

**3. Дискуссия**

Тема дискуссии: Понятие информационного общества и его особенности.

Перечень вопросов для проведения дискуссии:

Соотношение информации и данных в правоприменении.

**4. Компетентностно-ориентированная задача (ситуационная)**

# Анисимов работал и занимал различные должности в отделе технической поддержки UNIX Общества с ограниченной ответственностью (далее ООО) «Приват Трейд». С Анисимовым было заключено соглашение о конфиденциальности для работников ООО «Приват Трейд», согласно которого конфиденциальной информацией является техническая, технологическая, коммерческая (финансовая), организационная или иная используемая в коммерческой деятельности информация, которая обладает действительной или потенциальной коммерческой ценностью в силу ее неизвестности неограниченному кругу третьих лиц, и к которой нет свободного доступа на законном основании.

# В период с 2015 по 2016 годы Анисимов, находясь на своем рабочем месте, используя средства авторизации (логин и пароль), предоставленные ООО «Приват Трейд», и имея, в силу исполняемых обязанностей, доступ к информационным носителям, на которых содержится охраняемая компьютерная информация, скопировал на USB - носитель информацию из базы данных ООО «Приват Трэйд», а именно: не менее 40.000 записей, содержащих не прошедших проверку имен, фамилий, никнеймов (имена, которые используется при регистрации на интернет сайтах), а так же адресов электронной почты. После чего Анисимов передал вышеуказанную информацию Мусалову, который не был осведомлен о том, что полученная им информация охраняется внутренними документами ООО «Приват Трэйд».

# Задание. Оцените действия Анисимова и Мусалова с правовых позиций действующего законодательства.

# Тема 2. Информационно-коммуникационные технологии

**План занятия:**

1. Информационные технологии в сфере правовых отношений: этапы развитие.

2. Развитие информационных и коммуникационных технологий как фактор развития общества.

3. Информационные системы в области правоохранительной деятельности, государственного управления и информационной безопасности.

4. Информационные системы: структура и классификация.

5. Государственная система распространения правовой информации.

**Задания:**

**1. Доклад**

Тема доклада:

Государственные информационные системы.

**2. Реферат**

Тема реферата:

Система электронного опубликования нормативных актов и их проектов.

**3. Дискуссия**

Тема дискуссии: История развития правовой информатики в России и за рубежом.

Перечень вопросов для проведения дискуссии:

Соотношение развития и использования телекоммуникационных технологий в РФ и за рубежом.

**4. Компетентностно-ориентированная задача (ситуационная)**

Исследователи неоднократно поднимали вопрос о потенциальной угрозе национальной безопасности России, реализованной в социальных сетях. Экстремистские группы социальных сетей представляют реальную угрозу национальной безопасности страны, вовлекая до миллиона молодых граждан России, пропагандируя идеи политического экстремизма, национального и гендерного превосходства и неравенства. Подобных групп в социальных сетях немало и, если какие-то из них блокируются техническими службами по заявлениям неравнодушных пользователей, то на их месте появляется множество других с таким же опасным контентом.

Задание. Используя инверсионный анализ, предложите меры по защите подрастающего поколения от негативного информационного воздействия экстремистских групп на примере социальной сети «ВКонтакте».

**Тема 3. Компьютерные системы обмена информацией в профессиональной деятельности**

**План занятия:**

1. Компьютерные сети.

2. Типы компьютерных сетей, их топология.

3. Физическая и логическая топология компьютерных сетей.

4. Базовые топологии компьютерных сетей.

5. Адреса информации в Интернете (числовой адрес компьютера, доменное имя компьютера, URL-адрес документа).

**Задания:**

**1. Доклад**

Тема доклада:

Сеть Интернет как глобальный информационный ресурс.

**2. Реферат**

Тема реферата:

Средства и устройства сетевого обмена цифровой информацией: телефонная сеть и модем, удаленный и мобильный доступ, провайдер Интернета.

**3. Дискуссия**

Тема дискуссии: Возможности использования информационных и телекоммуникационных технологий в профессиональной деятельности.

Перечень вопросов для проведения дискуссии:

Веб-технологии в Интернете и локальной сети.

**4. Компетентностно-ориентированная задача (ситуационная)**

Платежи физических лиц в настоящее время все чаще производятся с помощью смартфонов через личный профиль интернет-банка. Подтверждение платежей физическим лицом происходит через одноразовые пароли, высылаемые на привязанный номер мобильного оператора смс-сообщением.

Задание. Определите уязвимости данной системы, используя методы инверсионного анализа.

**Тема 4. Правовые вопросы обеспечение информационной безопасности**

**План занятия:**

1. Общие вопросы информационных прав и свобод человека и гражданина.

2. Особенности обеспечения информационной безопасности в различных сферах жизни общества.

3. Правонарушение в информационной сфере, состав правонарушения.

**Задания:**

**1. Доклад**

Тема доклада:

Сущность конституционного права на информацию и его гарантии.

**2. Реферат**

Гражданская, административная, уголовная, дисциплинарная и иные виды ответственности за правонарушения в информационной сфере.

**3. Дискуссия**

Тема дискуссии: Информационные прав и свобод человека и гражданина.

Перечень вопросов для проведения дискуссии:

Права на информацию и свободы доступа к информации – и их развития в современном, информационном обществе.

**4. Компетентностно-ориентированная задача (ситуационная)**

ООО «Холдинг-М» в лице Москвина осуществляло предоставление возмездных Интернет услуг с применением 2-х электронных терминалов «Инфоинтсэйл», на жестких дисках которых установлены и использовались для работы терминала два экземпляра программы для ЭВМ «Microsoft Windows XP Professional», обладателем авторских и смежных прав на которую является «Корпорация Microsoft».

Вышеуказанные экземпляры ЭВМ являются контрафактными по следующими признакам: отсутствуют документы, подтверждающие приобретение копии программы «Microsoft Windows XP Professional»; в корпусе системного блока не имеется сертификата подлинности программы (СОА) с наименованием и уникальным буквенно-цифровым ключом программного продукта; отсутствует соглашение с правообладателем об участии в программе корпоративного лицензирования, тем самым ООО «Холдинг-М» использовало с целью получения прибыли программу для ЭВМ «Microsoft Windows XP Professional». Представитель ООО «Холдинг- М» Москвин пояснял, что документов, подтверждающих приобретение обществом операционной «Windows XP» у него не имеется.

Задание. Оцените ситуацию с точки зрения авторского права.

**Тема 5. Защита и обслуживание информации в компьютерных системах.**

**План занятия:**

1. Информационная безопасность. Понятие «защита информации»

2. Классификация мер и принципы защиты информации.

3. Категории защищаемой информации.

4. Угрозы, риски и пути утечки компьютерной информации.

5. Основы защиты информации и сведений, составляющих государственную тайну.

**Задания:**

**1. Доклад**

Тема доклада:

Парольная защита.

**2. Реферат**

Тема реферата:

Приемы защиты информации. Разграничение доступа, преобразование информации к нечитаемому виду (архивация, кодирование, шифрование).

**3. Дискуссия**

Тема дискуссии: Электронная подпись.

Перечень вопросов для проведения дискуссии:

Виды электронных подписей и правовая основа их использования.

**4. Компетентностно-ориентированная задача (ситуационная)**

Оператор ПК Абдуллин, согласно своим должностным обязанностям, приеме электронных носителей с материалами обязан был проверять их на наличие вирусов. Пытаясь завершить работу как можно скорее, Абдуллин проигнорировал проверку на антивирусном программном обеспечении.

В результате попадания вируса в компьютерную систему был испорчен готовый к печати оригинал-макет выпуска газеты. Редакция понесла убытки, был нанесен репутационный вред изданию.

Задание. Оцените действия Абдуллина с точки зрения действующего законодательства.

**5. Лабораторная работа**

**Применение инверсионного метода для выявления уязвимостей информационной системы.**

Порядок выполнения работы

1. Изучить теоретические сведения, при необходимости обратиться к интернет-источникам

2. Изучить учебную задачу

3. Применить инверсионный метод для самостоятельного решения задач информационной безопасности.

**Краткие теоретические сведения.**

Инверсионный метод (Диверсионный анализ) — это один из разделов ТРИЗ (теории решения изобретательских задач - основоположник Альтшуллер Г.С.), направленный на выявление и предотвращение вредных явлений в системах различного генезиса – технических, информационных, организационных .

Суть метода состоит в инвертировании проблемной ситуации при выявлении технических противоречий в системе, то есть в создании системной диверсии.

Метод позволяет выявить явные и скрытые причины возможных отказов, уязвимостей, рисков, иных вредных явлений в системе, тем самым появляется возможность спрогнозировать и предотвратить проявление проблем такого рода, предусмотрев соответствующие меры при разработке или модификации системы. Таким образом, метод применяется:

• для поиска причин вредных явлений;

• для прогнозирования возможных вредных явлений.

Применительно к информационной системе, реализованной посредством информационно-коммуникационных технологий, задача состоит в ее «взломе» и несанкционированном доступе к информации.

Как правило, инверсионный метод реализуется через последовательные стадии:

1. Инвертирование задачи.

2. Формулирование «диверсионных гипотез».

3. Выявление «диверсионных ресурсов».

4. Тестирование «диверсионных гипотез».

В более сложных ситуациях может быть использован более широкий набор инструментов анализа .

Рассмотрим алгоритм решения учебной задачи с применением инверсионного метода и возможные схемы решений.

Учебная задача «Об электронной оболочке»: Необходимо определить перечень уязвимостей электронной оболочки личных профилей профессорско-преподавательского состава (далее - ППС) вуза, предложить меры по устранению потенциальных угроз.

Согласно ГОСТ Р 56545-2015 «уязвимость» - это недостаток (слабость) программного (программно-технического) средства или ИС в целом, который (которая) может быть использована для реализации угроз безопасности информации.

Информационная система - это совокупность содержащейся в базах данных (далее по тексту - БД) информации и обеспечивающих ее обработку информационных технологий и технических средств.

Стадия 1: Инвертирование задачи.

Переформулируем задачу в виде: «Как взломать электронную оболочку личных профилей ППС и получить доступ к конфиденциальной информации?»

Стадия 2: Формулирование диверсионных гипотез.

В вузе принят негласный шаблон составления логина профиля из фамилии и инициалов имени и отчества преподавателя. Таким образом, логин можно составить, исходя из сведений о фамилии, имени и отчества, данные сведения являются открытыми и доступны на сайте университета.

После определения логина, остается подобрать пароль.

Несложно просто подсмотреть пароль, либо при выполнении каких-либо работ попросить интересующего нас преподавателя войти в его профиль, ссылаясь на неработающий свой или какие-то неполадки системы. Этот способ допустим, если «добытчик» пароля является сотрудником и в силу своего должностного положения может осуществить описанную последовательность действий.

Если такая мера неосуществима, пароль можно вычислить, пользуясь специальным программным обеспечением. При известном логине, вычислительных ресурсов только «взлома» пароля требуется немного.

Существует множество программ, две наиболее популярные - аdvnced аrchive Pаssword Recovery и Visаul Zip Pаssword Recovery Processor.

Кроме вышеперечисленных способов

можно попытаться подобрать пароль с клавиатуры, используя известную информацию о человеке - день рождения, имя любимого питомца, и т.д.

Таким образом, предложены три диверсионные гипотезы для решения данной задачи.

Стадия 3: выявление диверсионных ресурсов.

На этой стадии необходимо составить список ресурсов, которые способствуют реализации диверсионных гипотез.

Перечень диверсионных ресурсов может быть таким:

• наличие шаблона составления логина;

• низкий уровень дисциплины ППС в области информационной безопасности;

• незнание и/или несоблюдение элементарных правил сохранения своих идентификаторов и аутентификаторов;

• малая обеспеченность компьютерной техникой рабочих мест ППС, когда за одним персональным компьютером закреплено несколько сотрудников.

Стадия 4: тестирование диверсионных гипотез - определение процедуры тестирования и проведение тестов.

Процедура тестирования состоит в экспериментальной проверке «взлома» электронной оболочки личных профилей ППС, то есть реализации выдвинутых гипотез на стадии 2.

Проверкой установлено, что логины были определены по шаблону «фамилия+инициалы». Среднее время определения логинов - 10 минут.

Подбор паролей с помощью программного обеспечения к трем профилям осуществлен в среднем в течение 30 минут, таким образом, тестирование подтвердило правоту диверсионных гипотез и наличие уязвимостей в описанной информационной системе.

При подведении итогов решения учебной задачи были предложены следующие способы усиления информационной защиты электронной оболочки:

• рекомендация замены логина и пароля пользователя после первого входа и

активации профиля;

• разработка инструкции для сотрудников о необходимости сохранения аутентификаторов и идентификаторов;

• регулярный инструктаж сотрудников по соблюдению правил обеспечения информационной безопасности системы.

**6. Тесты**

**2. ВНЕАУДИТОРНАЯ КОНТАКТНАЯ РАБОТА ПРЕПОДАВАТЕЛЯ С ОБУЧАЮЩИМИСЯ ПО ДИСЦИПЛИНЕ «ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ»**

В течение периода изучения дисциплины преподаватель обеспечивает процесс освоения материла обучающимся не только в аудиторное время (лекции, практические (семинарские) занятия), но и во внеаудиторное время.

Виды внеаудиторной работы соответствуют учебному плану и рабочей программе дисциплины на текущий учебный год.

С этой целью преподаватель проводит консультации обучающихся по дисциплине «Информационно-коммуникационные технологии и информационная безопасность в юридической деятельности» и по результатам ее изучения – зачет. При этом преподавателем учитываются степень освоения обучающимся знаний, полученных как при его контактной работе с преподавателем, так и при его самостоятельной работе, в том числе ответы на практических занятиях, решения компетентностно-ориентированных задач, активность в дискуссиях, качество подготовки рефератов, посещаемость.

 Зачет служит формой проверки успешного усвоения обучающимся учебного материала лекционных, семинарских (практических) занятий. Преподаватель оценивает степень сформированности компетенций на этапе изучения данной дисциплины. Зачет для обучающихся всех форм обучения могут проводится в письменной или устной форме. Допускается проводить зачет в форме тестирования. На зачете обучающемуся могут быть заданы дополнительные вопросы в рамках рабочей учебной программы дисциплины.

Вопросы к зачету соответствуют рабочей программе дисциплины на текущий учебный год.

Знания, полученные при освоении дисциплины «Информационно-коммуникационные технологии и информационная безопасность в юридической деятельности», могут быть применены обучающимся при подготовке выпускной квалификационной работы

**Приложение 1**

**РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА**

**Основная учебная и научная литература**

1. Ельчанинова, Н. Б. Информационные технологии в юридической деятельности: Учебное пособие / Ельчанинова Н.Б. – Таганрог : Южный федеральный университет, 2016. - 128 с.: ISBN 978-5-9275-2197-5. - Текст : электронный. - URL: <https://znanium.com/catalog/product/994845>
2. Основы информационных технологий : учебное пособие / С. В. Назаров, С. Н. Белоусова, И. А. Бессонова [и др.]. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 530 c. — ISBN 978-5-4497-0339-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <https://www.iprbookshop.ru/89454.html>
3. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2021. — 180 с. — (Научная мысль). — DOI 10.12737/monography\_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1137902>
4. Баранова, Е. К. Информационная безопасность. История специальных методов криптографической деятельности : учебное пособие / Е. К. Баранова, А. В. Бабаш, Д. А. Ларин. - Москва : РИОР : ИНФРА-М, 2020. - 236 с. - ISBN 978-5-369-01788-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1118462

**Дополнительная учебная и научная литература**

1. Основы информационных технологий : учебное пособие / С. В. Назаров, С. Н. Белоусова, И. А. Бессонова [и др.]. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 530 c. — ISBN 978-5-4497-0339-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <https://www.iprbookshop.ru/89454.html>
2. Информационные технологии в юридической деятельности : учебное пособие для студентов вузов, обучающихся по специальностям «Юриспруденция» и «Правоохранительная деятельность» / С. Я. Казанцев, Н. М. Дубинина, А. И. Уринцов [и др.] ; под редакцией А. И. Уринцова. — 2-е изд. — Москва : ЮНИТИ-ДАНА, 2020. — 352 c. — ISBN 978-5-238-03242-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <https://www.iprbookshop.ru/109189.html>
3. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 c. — ISBN 978-5-4497-0338-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <https://www.iprbookshop.ru/89453.html>
4. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 c. — ISBN 978-5-4497-0675-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <https://www.iprbookshop.ru/97562.html>
5. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности : учебное пособие / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 431 c. — ISBN 978-5-4497-0935-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102070.html

**Нормативные и иные правовые акты, официальные акты высших судебных органов (в действующей редакции):**

1. Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 года // Российская газета. 1993. 25 декабря.
2. Федеральный закон от 17 января 1992 г. № 2202-I «О прокуратуре Российской Федерации» // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации от 20 февраля 1992. № 8, Ст. 366.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (действующая редакция) // Парламентская газета. № 241-242, 22.12.2001. Российская газета. № 249, 22.12.2001. Собрание законодательства РФ. 24.12.2001. № 52 (ч. I). Ст. 4921. Ведомости Федерального Собрания РФ. 01.01.2002. № 1. ст. 1.
4. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (действующая редакция) // Собрание законодательства РФ. 17.06.1996. № 25. Ст. 2954. Российская газета. № 113. 18.06.1996. № 114. 19.06.1996. № 115. 20.06.1996. № 118. 25.06.1996.

О прокуратуре Российской Федерации (ред. от 28.11.2015) [Электронный ресурс]: Федеральный закон от 17.01.1992 г. № 2202-1-ФЗ. – Режим доступа: www.consultant.ru/document/cons\_doc\_LAW

О Следственном комитете Российской Федерации (ред. от 30.12.2015) [Электронный ресурс]: Федеральный закон от 28 декабря 2010. № 403-ФЗ. – Режим доступа: www.consultant.ru/document/cons\_doc\_LAW\_108565

1. Гражданский кодекс Российской Федерации. (Часть первая) от 30 ноября 1994 года // СЗ РФ. 1994. № 32. Ст. 3301.
2. Гражданский кодекс Российской Федерации. (Часть вторая) от 26 января 1996 г. № 14-ФЗ //СЗ РФ. 1996. № 5. Ст. 410.
3. Федеральный закон от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» // СЗ РФ. 2001. № 23. Ст. 2291.
4. Гражданский кодекс Российской Федерации. (Часть третья) от 26 ноября 2001 г. № 146-ФЗ // СЗ РФ 2001. № 49. Ст. 4552.
5. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ // СЗ РФ. 2002. № 1 (часть I). Ст. 3.
6. Федеральный закон от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» // СЗ РФ. 2002. № 23. Ст. 2102.
7. Гражданский процессуальный кодекс РФ от 14 ноября 2002 г. № 138-ФЗ // СЗ РФ. 2002. № 46. Ст. 4532.
8. Гражданский кодекс Российской Федерации. (Часть четвёртая) от 18 декабря 2006 г. № 230-ФЗ // СЗ РФ. 2006. № 52 (часть I). Ст. 5496.

**Приложение 2**

**РЕКОМЕНДУЕМЫЕ ИНТЕРНЕТ– САЙТЫ**

1. Официальный интернет-портал правовой информации <http://www.pravo.gov.ru/ips/>.
2. Научно-технический центр правовой информации "Система" Федеральной службы охраны Российской Федерации <http://www1.systema.ru/>.
3. Официальный сайт МВД России – [www.мвд.рф](http://www.мвд.рф)
4. Официальный сайт Следственного комитета Российской Федерации – [www.sledcom.ru](http://www.sledcom.ru)

**Приложение 3**

**Перечень современных профессиональных баз данных и информационных справочных и поисковых систем**

1. Государственная автоматизированная система Российской Федерации «Правосудие» https://sudrf.ru/
2. Справочная информация по делам ВС РФ - <https://vsrf.ru/lk/practice/cases>
3. Справочная информация по жалобам - <https://vsrf.ru/lk/practice/appeals>
4. Правовая система «КонсультантПлюс» // Сайт «Consultant.ru» [Электронный ресурс] – URL: <http://www.consultant.ru>
5. Справочно-правовая система «Гарант» // Сайт «Aero.garant.ru» [Электронный ресурс] – URL: <http://www.aero.garant.ru>
6. Судебные и нормативные акты РФ // Сайт «Sudact.ru» [Электронный ресурс] – URL: <https://sudact.ru>
7. Генеральная прокуратура РФ. Портал правовой статистики <http://crimestat.ru/>
8. Банк данных "Нормативно-правовые акты, зарегистрированные в Министерстве юстиции Российской Федерации" // Сайт Министерства юстиции РФ [Электронный ресурс] – URL:https://minjust.consultant.ru/
9. Реферативная и цитируемая база рецензируемой литературы «Scopus» <https://www.scopus.com>
10. Реферативные базы данных публикаций в [научных журналах](https://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D1%83%D1%87%D0%BD%D1%8B%D0%B9_%D0%B6%D1%83%D1%80%D0%BD%D0%B0%D0%BB) и [патентов](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%82%D0%B5%D0%BD%D1%82) «Web of Science» <http://apps.webofknowledge.com>
11. Научная электронная библиотека «eLIBRARY.RU» <https://elibrary.ru>
12. Сайт Российской государственной библиотеки <https://www.rsl.ru>
13. Поисковая система «Яндекс» <https://yandex.ru/>
14. Поисковая система «Google» <https://www.google.ru/>

**ОГЛАВЛЕНИЕ**

ВВЕДЕНИЕ ………………………………………………………........3

1. АУДИТОРНАЯ КОНТАКТНАЯ РАБОТА ПРЕПОДАВАТЕЛЯ

С ОБУЧАЮЩИМИСЯ ПО ДИСЦИПЛИНЕ

«ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ»………………………………4

1. ВНЕАУДИТОРНАЯ КОНТАКТНАЯ РАБОТА ПРЕПОДАВАТЕЛЯ С ОБУЧАЮЩИМИСЯ ПО ДИСЦИПЛИНЕ

«ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ»……………………………..14

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА……………………………….16

РЕКОМЕНДУЕМЫЕ ИНТЕРНЕТ–САЙТЫ………………….........19

Перечень современных профессиональных баз данных и информационных справочных и

поисковых систем....................................................................19

**ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ**

*Методические указания*

Составитель: **Помазанов** Виталий Викторович, **Грицаев** Сергей Иванович

Подписано в печать 00.00. Формат 60 × 84 1/16.

Усл. печ. л. – 0. Уч.– изд. л. – 0.

Тираж 000 экз. Заказ №000

Типография Кубанского государственного

аграрного университета.

350044, г. Краснодар, ул. Калинина, 13