Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

Кафедра прикладной информатики

Методические рекомендации для обучающихся по освоению дисциплины

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Основная профессиональная образовательная программа
высшего образования по направлению подготовки

40.03.01 Юриспруденция

Направленность (профиль):
Правовое регулирование деятельности Северного морского пути

Уровень:
Бакалавриат

Форма обучения
Очная

Рассмотрен и утвержден на заседании кафедры
4 06 2021 г., протокол № 7
Зав. кафедрой Истомин Е.П.

Авторы-разработчики:
Сидоренко А.Ю.

Санкт-Петербург 2021

1. Планирование и организация времени, необходимого для изучения дисциплины

Дисциплина «Информационные технологии в юридической деятельности» в соответствии с учебным планом по направлению 40.03.01 - Юриспруденция изучается во первом семестре первого курса по очной форме обучения. Объем дисциплины составляет 4 зачетных единицы, 144 академических часа, из них на занятия лекционного типа отводится 28 часов, на практические занятия – 28 часов, на самостоятельную работу – 88 часа.

Программой дисциплины предусмотрено проведение лекционных занятий, на которых дается основной систематизированный материал, и практических занятий, предполагающих закрепление изученного материала и формирование у обучающихся необходимых знаний, умений и навыков.

2. Рекомендации по контактной работе

Залогом успешного освоения дисциплины является обязательное посещение лекционных и практических занятий, так как пропуск одного (тем более, нескольких) занятий может осложнить освоение тематических разделов дисциплины.

2.1. Работа на лекциях

Для успешного овладения дисциплиной необходимо выполнять следующие требования:

- посещать все лекционные занятия, для качественного усвоения знаний по дисциплине;
- все рассматриваемые на лекциях темы и вопросы обязательно фиксировать (либо на бумажных, либо на машинных носителях информации);
- обязательно выполнять все домашние задания, получаемые на лекциях для подготовки к практическим занятиям;
- проявлять активность на интерактивных лекциях и при подготовке к ним;
- в случаях пропуска занятий по каким-либо причинам, необходимо обязательно самостоятельно изучать соответствующий материал.

2.2. Работа на практических занятиях

На практических занятиях материал, изложенный на лекциях, закрепляется при проведении опросов, а также в рамках выполнения практических заданий.

3. Рекомендации по самостоятельной работе

3.1. Подготовка к практическим занятиям

На практическом занятии вырабатываются, углубляются и развиваются самостоятельность мышления, умение делать выводы, связывать теоретические положения с практикой, навыки публичных выступлений, развивается культура речи и умение полемизировать. Подготовка к занятию начинается заблаговременно. Прежде всего, необходимо сразу же после лекций (но не позднее одного-двух дней после того, как она прослушана) перечитать свой конспект, расшифровать сокращенные записи и внести необходимые поправки и дополнения. Одновременно изучается соответствующий раздел учебника и рекомендованная литература.

Заканчивается подготовка к практическому занятию составлением краткого конспекта, в котором отражаются все вопросы, выносимые на очередное занятие.

При подготовке к практическим занятиям в рамках самостоятельной работы по изучению дисциплины обучающимся необходимо:

– повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной по данной теме литературы;

– подготовиться по вопросам, предложенным для проверки знаний, а также вынесенным на обсуждение;

– при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники;

– выполнить практические задания в рамках изучаемой темы;

– подготовиться к промежуточной аттестации.

3.2. Подготовка к текущему контролю

3.2.1. Методические указания по подготовке к устному опросу.

Устный опрос студента является одной из форм текущего контроля. Устный опрос студента направлен на поиск правильных ответов по темам дисциплины, закрепление изученного лекционного материала, а также на приобретение у студента навыка аргументированно вести полемику, отстаивать сформулированную точку зрения. Устный опрос студента в присутствии других студентов способствуют лучшему усвоению изучаемого материала, а также применению других форм текущего контроля (тематические обсуждения и дискуссии). В результате устного опроса студент должен дать аргументированный развернутый ответ на поставленный преподавателем вопрос. Примеры вопросов для устного опроса представлены в Фонде оценочных средств по дисциплине.

Образцы вопросов для устного опроса

1. Что такое информация и каковы её свойства?
2. Каковы основные черты информационного общества?
3. Как информационные технологии помогают оптимизировать юридическую деятельность?
4. В какой форме представлена информация в компьютере?
5. В чём преимущества сетевой организации информационных систем?
6. Операционная система и её функции.
7. Назовите основные сетевые топологии.
8. Назовите принципы архитектуры фон Неймана.
9. Какие основные узлы компьютера расположены на материнской плате?
10. Какие носители и накопители информации вам известны?
11. Какова роль системного программного обеспечения в функционировании компьютера?
12. Как организована файловая структура компьютера?
13. Раскройте содержание понятий: символ, слово, абзац, страница, раздел, разметка документа.

Критерии оценивания задания репродуктивного уровня

Правильность и четкость ответа
Отсутствие ошибок, оговорок
Четкость и грамотность речи
Раскрытие содержания вопроса
Полнота ответа: знание определений понятий, основных положений, рассмотрение различных точек зрения (если вопрос предполагает, характеристика концепций (положений) разных авторов)
Установление внутрипредметных и межпредметных связей
Собственный анализ и оценка излагаемого материала (если вопрос предполагает, сопоставление концепций (положений) разных авторов), примеры, раскрытие возможных противоречий, проблем, их оценка

3.2.2. Методические указания по подготовке к практическим заданиям.

Практические задания являются одной из форм текущего контроля, их цель - обеспечить контроль знаний студента по темам дисциплины. Примеры практических заданий представлены в Фонде оценочных средств по дисциплине. Приступать к выполнению практических заданий без изучения основных положений и понятий науки, не следует, так как в этом случае студент, как правило, плохо ориентируется в материале, не может отграничить смежные вопросы и сосредоточить внимание на основных,

первостепенных проблемах рассматриваемой темы.

Образцы практических заданий текущего контроля

1. Цифровая подпись

Цифровая подпись (digital signature) - это способ проверки целостности содержимого сообщения и подлинности его отправителя. Она реализуется при помощи асимметричных шифров и хэш-функций. Цифровая подпись основана на обратимости асимметричных шифров, а также на взаимосвязанности содержимого сообщений, самой подписи и пары ключей: изменение одного из этих элементов сделает невозможным подтверждение подлинности подписи.

Отправитель вычисляет дайджест сообщения, шифрует его своим ключом и отправляет вместе с письмом. Получатель, приняв сообщение, расшифровывает дайджест открытым ключом отправителя. Кроме того, получатель сам вычисляет дайджест принятого сообщения и сравнивает его с расшифрованным. Если два дайджеста совпадают, то подпись является подлинной. В противном случае либо изменено содержание сообщения, либо подпись подделана.

Шифр RSA также используют для выработки и проверки цифровой подписи. Чтобы подписать сообщение, отправитель шифрует его дайджест своим личным секретным ключом – это и есть ЭП, и отправляет сообщение вместе с подписью и открытым ключом. Получатель расшифровывает подпись открытым ключом отправителя, вычисляет дайджест принятого сообщения и сравнивает результаты. Если сообщение подлинное, то вычисленный и расшифрованный дайджесты должны совпадать.

1. Генерация ключей

Создать пары ключей с помощью чисел $p_1 = 3$; $q_1 = 11$ для оппонента А и $p_2 = 5$; $q_2 = 7$ для оппонента Б.

Общий алгоритм генерации открытого и секретного ключей:

- возьмем два простых числа p и q. Оппонент А выбирает p = 3; q = 11. Оппонент Б: p = 5; q = 7;
- определим **N**, как результат умножения N= p*q;
- определим **M**, как результат умножения M = (p-1)*(q-1);
- выберем простое число, которое назовем **d**. Это число должно быть взаимно простым (не иметь ни одного общего делителя, кроме 1) с числомM;
- определим такое число **b**, для которого является истинным следующее соотношение (b*d) mod M=1;
- назовем **открытым ключом пару чисел {b;N}, а секретным –{d;N};**
- пары чисел внесем в соответствующие таблички на листе Excel.

2. Корреспондентам обменяться открытыми ключами. Секретные сохранить в файле.

Теперь с помощью полученной пары ключей можно создать цифровую подпись сообщения. При этом дайджест (см. п.3) сообщения должен шифроваться **секретным ключом отправителя**, а расшифровываться **открытым ключом отправителя.**

Для того чтобы в дальнейшем зашифровать дайджест секретным ключом *{d, N},* необходимо следующее:

- вычислить дайджест сообщения D (см. п. 3);
- зашифровать дайджест **своим секретным ключом**, , по формуле

S = (D^d) mod N.

- подписать свое письмо подписью S и отправить письмо оппоненту.

Чтобы расшифровать **ЭП под письмом Вашего оппонента**, используйте открытый **ключ оппонента *{d, N},*** для этого необходимо выполнить следующие вычисления: *D = (S^b) mod N*.

В результате будет получено число D, которое представляет собой дайджест сообщения оппонента.

3. Создание дайджеста сообщения и ЭП

Хэш-функцией называется алгоритм, конвертирующий строку произвольной длины

(сообщение) в битовую строку фиксированной длины, называемой хэш-кодом, проверочной суммой или цифровым отпечатком. Хеширование (иногда «хэширование», англ. hashing) — преобразование по детерминированному алгоритму входного массива данных произвольной длины в выходную битовую строку фиксированной длины. Такие преобразования также называются хеш-функциями или функциями свёртки, а их результаты называют хешем, хеш-кодом или дайджестом (англ. Message digest).

Хеширование применяется для построения ассоциативных массивов, поиска дубликатов в сериях наборов данных, построения достаточно уникальных идентификаторов для наборов данных, контрольного суммирования с целью обнаружения случайных или намеренных ошибок при хранении или передаче, для хранения паролей в системах защиты (в этом случае доступ к области памяти, где находятся пароли, не позволяет восстановить сам пароль)**, при выработке электронной подписи.**

Порядок создания дайджеста сообщения D:

3.1. Каждому абоненту создать сообщение длиной не менее 20 литер. Придумайте что-нибудь пооригинальнее, чем «Привет …». Это сообщение - оригинал, впишите его в столбик по литере в каждую ячейку по вертикали. В соседнем столбце отобразите числовой код литер в соответствии с таблицей кодировки Windows-1251, для этого нужно воспользоваться функцией ВПР().

3.2. Хэш-функцию сформируем следующим образом: [сумма всех числовых кодов сообщения] mod K

где K – максимальное простое число < N.

D = ∑[числовые коды литер сообщения] mod K

Хэш-функция должна быть одинакова у отправителя и получателя, поэтому число К у них одинаково. Для вычисления дайджеста воспользоваться функцией ОСТАТ().

3.3. Зашифруем дайджест своим секретным ключом. Для этого также понадобится функция ОСТАТ(). Полученное число является ЭП автора сообщения.

4. Передача сообщения.

Вставим текст сообщения в письмо. Добавим к сообщению полученную свою ЭП и открытый ключ.

5. Подтверждение подлинности.

Вычислим дайджест полученного сообщения по правилу, изложенному в п. 3.2.

Расшифруем ЭП, полученную в письме, **открытым ключом отправителя** и сравним результаты. Совпадение дайджестов подтверждает подлинность сообщения.

В своем сообщении изменить текст, хотя бы одну букву. Обратите внимание, как меняется дайджест и ЭП. Т.е. ЭП уникальна для каждого документа или сообщения.

Критерии оценивания ситуационной задачи

Критерий	**Оценка**
Работа выполнена без замечаний, на поставленные вопросы есть качественный ответ	5
Работа выполнена без замечаний, на поставленные вопросы нет корректного ответа	4
Работа выполнена с замечаниями, на поставленные вопросы есть качественный ответ	3
Работа не выполнена. На поставленный вопрос нет ответа.	2

3.3. Подготовка к промежуточной аттестации.

3.3.1. Методические указания по подготовке к экзамену.

Изучение дисциплины завершается экзаменом.

В процессе подготовки к экзамену студенты должны обратиться к изученному на лекциях и практических занятиях учебному материалу, конспектам лекций, рекомендованным преподавателями курса учебникам, иным информационным ресурсам,

учебным пособиям, монографиям и справочникам. Студенты также должны ориентироваться на новейшие научные источники информации, в том числе статьи в соответствующих профильных журналах. Знания студентов, определяемые на зачете, должны быть систематизированы и логически осмыслены.

Перечень вопросов для подготовки к зачету:

1. Что такое информация и каковы её свойства?
2. Каковы основные черты информационного общества?
3. Как информационные технологии помогают оптимизировать юридическую деятельность?
4. В какой форме представлена информация в компьютере?
5. В чём преимущества сетевой организации информационных систем?
6. Операционная система и её функции.
7. Назовите основные сетевые топологии.
8. Назовите принципы архитектуры фон Неймана.
9. Какие основные узлы компьютера расположены на материнской плате?
10. Какие носители и накопители информации вам известны?
11. Какова роль системного программного обеспечения в функционировании компьютера?
12. Как организована файловая структура компьютера?
13. Раскройте содержание понятий: символ, слово, абзац, страница, раздел, разметка документа.
14. Назовите основные этапы создания текстового документа.
15. Стандартные приложения Windows: Блокнот, WordPad, командная строка.
16. Текстовый процессор Word: работа с окнами, абзацами, шрифтами.
17. Текстовый процессор Word: режим структуры, работа со стилями, создание таблиц.
18. Что такое база данных? Что такое поле и запись?
19. Электронные таблицы. Основные понятия.
20. Содержание электронной таблицы: формулы, ссылки, копирование содержимого, автозаполнение.
21. В чём различие относительных и абсолютных адресов в табличном процессоре Excel?
22. Электронный документооборот: основные понятия. Для чего нужна электронная подпись?
23. Глобальная сеть Internet. Протокол TCP/IP.
24. Основные службы системы Internet. Протокол HTTP.
25. Технологии подключения к Internet.
26. Электронная почта. Структура сообщений электронной почты.
27. Автоматизированные информационные системы и банки данных. Экспертные системы.
28. Электронный документ. Принцип электронной подписи.
29. Электронная подпись как криптографическая система.
30. Электронный документооборот: основные понятия.
31. Электронные деньги.
32. Электронная почта. Структура сообщений электронной почты.
33. ПК-7
34. Правовая информационная система "КонсультантПлюс". Основные характеристики.
35. Методы поиска информации в системе "КонсультантПлюс".
36. Автоматизированные информационные системы и банки данных. Экспертные системы.

37. Какие основные виды вирусов вам известны?
38. Что такое DDOS-атака?

4. Работа с литературой

№	Раздел / тема дисциплины	Основная литература	Дополнительная литература
1	Тема 1. Основы информационных технологий. Компьютер как средство обработки информации	1. Информационные технологии в юридической деятельности: учебник для вузов / П. У. Кузнецов [и др.]; под общей редакцией П. У. Кузнецова. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-02598-9. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449842 2. Информационные технологии в юридической деятельности: учебник и практикум для академического бакалавриата / В. Д. Элькин [и др.] ; под редакцией В. Д. Элькина. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2019. — 403 с. — (Высшее образование). — ISBN 978-5-9916-5283-4. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/431764 3. Серова, Г. А. Информационные технологии в юридической деятельности: учебное пособие / Г. А. Серова. — Москва: ИНФРА-М, 2020. — 241 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-014579-2. - Текст: электронный. - URL: https://znanium.com/catalog/product/1057953 4. Внуков, А. А. Защита информации: учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2019. — 240 с. — (Высшее образование). — ISBN 978-5-534-01678-9. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/444046	1. Федотова Е.Л. Информационные технологии в профессиональной деятельности [Электронный ресурс]: Учебное пособие / - М.: ИД ФОРУМ: НИЦ Инфра-М, 2012. - 368 с. - Режим доступа: http://znanium.com/bookread2.php?book=322029 (ЭБС Знаниум). 2. Гаврилов, М. В. Информатика и информационные технологии: учебник для вузов / М. В. Гаврилов, В. А. Климов. — 4-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2020. — 383 с. — (Высшее образование). — ISBN 978-5-534-00814-2. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449779 3. Терещенко, Л. К. Модернизация информационных отношений и информационного законодательства: Монография / Л.К. Терещенко. - Москва: НИЦ ИНФРА-М: ИЗиСП, 2013. - 227 с. ISBN 978-5-16-006123-8. - Текст: электронный. - URL: https://znanium.com/catalog/product/442472
2	Тема 2. Аппаратное обеспечение информационных технологий		
3	Тема 3. Программное обеспечение информационных технологий		
4	Тема 4. Стандартные приложения операционной системы Windows. Текстовые редакторы		
5	Тема 5. Обработка документов средствами электронных таблиц. Работа с базами данных		
6	Тема 6. Основы электронного документооборота		
7	Тема 7. Получение информации из глобальной сети Интернет. Проблемы компьютерной безопасности		