



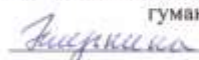
«Дальневосточный филиал Федерального государственного бюджетного
образовательного учреждения высшего образования
«Всероссийская академия внешней торговли
Министерства экономического развития Российской Федерации»

КАФЕДРА «ЕСТЕСТВЕННЫЕ И СОЦИАЛЬНО-ГУМАНИТАРНЫЕ НАУКИ»



«УТВЕРЖДЕНО»
решением Ученого совета
«ДВФ ВАВТ
Минэкономразвития России»
Протокол № 2 от «09» 06 2020 г.

«ОДОБРЕНО»
НМС «ДВФ ВАВТ
Минэкономразвития России»
Протокол № 11 от «04» 06 2020 г.
Председатель НМС
 Н.Г.Семикова

Утверждено
на заседании кафедры
«Естественные и социально-гуманитарные
науки»
Протокол № 9 от «28» 05 2020 г.
Зав. кафедрой «Естественные и социально –
гуманитарные науки»
 Т.А.Князькина

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

направление подготовки 40.03.01 «Юриспруденция»

направленность (профиль) «Гражданско-правовой»

уровень бакалавриата

факультатив

форма обучения (очная, очно-заочная, заочная)

Рабочая программа по дисциплине «Информационная безопасность, защита персональных данных» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования, утвержденным приказом Министерства образования и науки Российской Федерации № 1511 от 01.12.2016 г., Приказом Минобрнауки Российской Федерации от 05 апреля 2017 г. № 301 «Об утверждении порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры» и рабочим учебным планом.

Составитель —Богданов Вадим Васильевич доктор физико-математических наук, старший научный сотрудник, преподаватель кафедры естественных и социально-гуманитарных наук «Дальневосточного филиала федерального государственного бюджетного образовательного учреждения высшего образования «Всероссийская академия внешней торговли Министерства экономического развития Российской Федерации».

СОДЕРЖАНИЕ

| | | |
|-----|---|----|
| 1. | Организационно-методический раздел | 3 |
| 2. | Распределение часов дисциплины по формам и видам работ | 6 |
| 3. | Структура и содержание теоретической части дисциплины | 8 |
| 4. | Структура и содержание практической части дисциплины | 10 |
| 5. | Методические указания по освоению дисциплины | 10 |
| 6. | Учебно-методическое обеспечение самостоятельной работы обучающихся | 13 |
| 7. | Перечень информационных технологий и программного обеспечения | 19 |
| 8. | Материально-техническое обеспечение дисциплины | 20 |
| 9. | Библиографический список | 21 |
| 10. | Оценочные средства | 24 |
| | <i>10.1 Паспорт фонда оценочных средств</i> | 25 |
| | <i>10.2 План-график проведения контрольно-оценочных мероприятий</i> | 25 |
| | <i>10.3. Контрольные вопросы, выносимые на экзамен</i> | 25 |
| | <i>10.4. Темы рефератов, докладов</i> | 26 |
| | <i>10.5 Тестовые задания</i> | 27 |
| | <i>10.6 Критерии оценки знаний студентов</i> | 37 |
| 11 | Лист внесения изменений в рабочую программу учебной дисциплины | 41 |

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Рабочая программа дисциплины (далее - РП) «Информационная безопасность, защита персональных данных» разработана для студентов, обучающихся по направлению подготовки 40.03.01 «Юриспруденция» (уровень бакалавриата), направленность (профиль) «Гражданско-правовой» в соответствии с требованиями ФГОС ВО по данному направлению.

Данная дисциплина является факультативной.

Общая трудоемкость освоения дисциплины составляет 1 зач. ед. 36 ч., Учебным планом предусмотрены

| Форма обучения | Лекции | Практические занятия | Самостоятельная работа |
|----------------|--------|----------------------|------------------------|
| Очная форма | 8 | 10 | 18 |
| Очно-заочная | 8 | 10 | 18 |
| Заочная | 2 | 4 | 30 |

Цель и задачи изучения дисциплины

Цель изучения дисциплины «Информационная безопасность, защита персональных данных» - дать студентам необходимые знания, умения и навыки в области современных информационных технологий, применяемых в настоящее время, а также защиты информации.

Задачи изучения дисциплины

- овладение теоретическими знаниями в области информационных технологий и обеспечения их безопасности, а также управления информационными ресурсами;
- приобретение прикладных знаний в области создания систем защиты информации, а также оптимизации моделей сложных процессов бизнеса;
- овладение навыками самостоятельного использования соответствующих инструментальных программных систем.

В результате изучения данной дисциплины у студентов формируется следующие компетенции.

Перечень сформированных компетенций в процессе освоения дисциплины

| Код и формулировка компетенции | Этапы формирования компетенции | |
|--|--------------------------------|---|
| владение основными методами, способами и средствами получения, | знать | Методы, способы и средства получения, хранения и переработки информации; компьютер как средством управления информацией |

| | | |
|---|---------|--|
| хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) | уметь | Получать, сохранять и перерабатывать информацию; работать с компьютером как средством управления информацией. |
| | владеть | основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией |
| Способность работать с информацией в глобальных компьютерных сетях ОК-4 | знать | вопросы административного и организационно-правового обеспечения защиты информации, основные системы защиты информации в России и в ведущих зарубежных странах, основные методологические положения защиты информации, основные программно-аппаратные средства защиты компьютеров и программ, общие вопросы обеспечения информационной безопасности при работе в сети, особенности защиты информации в СУБД. |
| | уметь | ограничивать использование ресурсов компьютера на основе раздельного доступа пользователей в операционную систему, организовывать регистрацию пользователей в сетевой операционной системе, организовывать защиту информации в локальной сети на уровнях входа в сеть и системы прав доступа, организовывать безопасную работу в Интернет и отправку почтовых сообщений в глобальной сети, использовать средства защиты данных от разрушающих программных воздействий компьютерных вирусов |
| | владеть | Навыками защиты персональных данных в информационных системах |
| способность работать на благо общества и государства (ОПК-2) | знать | Проблему информационной безопасности в мире, аспекты защиты информации, угрозы информационной безопасности, методы борьбы с ней; особенности защиты информации в компьютерных сетях; место и роль информационной безопасности и защиты данных в благополучии общества и государства |
| | уметь | Применять свои знания в области информационной безопасности и защиты данных на благо общества и государства |
| | владеть | Навыками работы в сфере информационной безопасности и защиты данных на благо общества и государства |

| | | |
|--|---------|--|
| Способность осуществлять предупреждение правонарушений, выявлять и устранять причины и условия, способствующие их совершению (ПК-11) | Знать | сущность и понятие информационной безопасности, характеристику ее составляющих; - место информационной безопасности в системе национальной безопасности страны; - источники угроз информационной безопасности и меры по их предотвращению; - жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи; - современные средства и способы обеспечения информационной безопасности; - современные способы посягательств на информационную безопасность организации, человека. |
| | Уметь | классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; - применять основные правила и документы системы сертификации Российской Федерации; - классифицировать основные угрозы безопасности информации; выявлять и устранять причины, следствием которых является потеря защиты информации и персональных данных |
| | Владеть | методами и средствами технической защиты информации. |

В рамках изучаемой дисциплины ведется воспитательная работа, направленная на удовлетворение потребностей и интересов обучающегося в соответствии с культурными ценностями, которая способствует формированию личности, способной самостоятельно решать профессиональные задачи и придерживаться активной гражданской позиции в обществе.

Целью воспитательной работы является профессионально-трудовое, гражданско-правовое, государственно-патриотическое, духовно-нравственное и гуманитарно-эстетическое воспитание, в рамках которых осуществляется формирование инструментальных и системных знаний и умений в рамках общекультурных, общепрофессиональных и профессиональных компетенций, позволяющих выпускнику успешно работать в избранной сфере профессиональной деятельности и быть востребованным на рынке труда.

2. РАСПРЕДЕЛЕНИЕ ЧАСОВ ДИСЦИПЛИНЫ ПО ФОРМАМ И ВИДАМ РАБОТ

Базовые разделы дисциплины и виды учебной работы, рекомендуемые для изучения студентам очной формы обучения

| № п/ п | Тема Дисциплины | Виды учебной работы, включая самостоятельную работу студентов | | | | | Формы текущего контроля успеваемости |
|--------------|---|--|-----|-----|-------|-----|--|
| | | всего | л/з | п/р | лаб/р | с/р | |
| 1 | Тема 1. Введение в проблему информационной безопасности. | 6 | 2 | 2 | | 2 | Реферат, доклад, тест |
| 2 | Тема 2. Правовые и организационные аспекты защиты информации. | 6 | 2 | 2 | | 2 | Реферат, доклад, тест |
| 3 | Тема 3. Угрозы информационной безопасности и методы их реализации. | 6 | 2 | 2 | | 2 | Реферат, доклад, тест |
| 4 | Тема 4. Методы и средства обеспечения информационной безопасности информационных систем | 6 | 2 | 2 | | 2 | Реферат, доклад, тест |
| 5 | Тема 5. Использование защищенных компьютерных систем. | 4 | | 2 | | 2 | Реферат, доклад, тест |
| 6 | Тема 6. Защита от разрушающих программных воздействий. | 2 | | | | 2 | Реферат, доклад, тест |
| 7 | Тема 7 Особенности защиты в операционных системах. | 2 | | | | 2 | Реферат, доклад, тест |
| 8 | Тема 8 Особенности защиты информации в компьютерных сетях. | 2 | | | | 2 | Реферат, доклад, тест |
| 9 | Тема 9. Защита программ и данных | 2 | | | | 2 | Реферат, доклад, тест |
| | | 36 | 8 | 10 | | 18 | зачет |

Базовые разделы дисциплины и виды учебной работы, рекомендуемые для изучения студентам очно-заочной формы обучения

| № п/ п | Тема Дисциплины | Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в з.ед./часах) | | | | | Формы текущего контроля успеваемости |
|--------------|---|--|-----|-----|-------|-----|--|
| | | всего | л/з | п/р | лаб/р | с/р | |
| 1 | Тема 1. Введение в проблему информационной безопасности. | 6 | 2 | 2 | | 2 | Реферат, доклад, тест |
| 2 | Тема 2. Правовые и организационные аспекты защиты информации. | 6 | 2 | 2 | | 2 | Реферат, доклад, тест |
| 3 | Тема 3. Угрозы информационной | 6 | 2 | 2 | | 2 | Реферат, доклад, |

| | | | | | | | |
|---|---|----|---|----|--|----|-----------------------|
| | безопасности и методы их реализации. | | | | | | тест |
| 4 | Тема 4. Методы и средства обеспечения информационной безопасности информационных систем | 6 | 2 | 2 | | 2 | Реферат, доклад, тест |
| 5 | Тема 5. Использование защищенных компьютерных систем. | 4 | | 2 | | 2 | Реферат, доклад, тест |
| 6 | Тема 6. Защита от разрушающих программных воздействий. | 2 | | | | 2 | Реферат, доклад, тест |
| 7 | Тема 7 Особенности защиты в операционных системах. | 2 | | | | 2 | Реферат, доклад, тест |
| 8 | Тема 8 Особенности защиты информации в компьютерных сетях. | 2 | | | | 2 | Реферат, доклад, тест |
| | Тема 9. Защита программ и данных | 2 | | | | 2 | Реферат, доклад, тест |
| | | 36 | 8 | 10 | | 18 | зачет |

Базовые разделы дисциплины и виды учебной работы, рекомендуемые для изучения студентам заочной формы обучения

| № п/п | Тема Дисциплины | Виды учебной работы, включая самостоятельную работу студентов | | | | | Формы текущего контроля успеваемости |
|-------|---|---|-----|-----|-------|-----|--------------------------------------|
| | | всего | л/з | п/р | лаб/р | с/р | |
| 1 | Тема 1. Введение в проблему информационной безопасности. | 5 | 2 | | | 3 | Реферат, доклад, тест |
| 2 | Тема 2. Правовые и организационные аспекты защиты информации. | 7 | | 4 | | 3 | Реферат, доклад, тест |
| 3 | Тема 3. Угрозы информационной безопасности и методы их реализации. | 3 | | | | 3 | Реферат, доклад, тест |
| 4 | Тема 4. Методы и средства обеспечения информационной безопасности информационных систем | 3 | | | | 3 | Реферат, доклад, тест |
| 5 | Тема 5. Использование защищенных компьютерных систем. | 3 | | | | 3 | Реферат, доклад, тест |
| 6 | Тема 6. Защита от разрушающих программных воздействий. | 3 | | | | 3 | Реферат, доклад, тест |
| 7 | Тема 7 Особенности защиты в операционных системах. | 3 | | | | 3 | Реферат, доклад, тест |
| 8 | Тема 8 Особенности защиты информации в компьютерных сетях. | 3 | | | | 3 | Реферат, доклад, тест |
| 9 | Тема 9. Защита программ и данных | 6 | | | | 6 | Реферат, доклад, тест |

| | | | | | | | |
|--|--|----|---|---|--|----|-------|
| | | 36 | 2 | 4 | | 30 | зачет |
|--|--|----|---|---|--|----|-------|

3. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ ДИСЦИПЛИНЫ

Тема 1. Введение в проблему информационной безопасности.

Программа информационной безопасности России и пути ее реализации. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ. Концепция информационной безопасности.

Обзор состояния систем защиты информации в России и в ведущих зарубежных странах. Международные стандарты информационного обмена.

Основные принципы защиты информации в компьютерных системах. Основные понятия и определения защиты информации.

Тема 2. Правовые и организационные аспекты защиты информации.

Современное состояние правового регулирования в информационной сфере. Правовое обеспечение информационной безопасности. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

Компьютерные преступления.

Организационное обеспечение информационной безопасности.

Тема 3. Угрозы информационной безопасности и методы их реализации.

Понятие угрозы. Анализ угроз безопасности информации. Причины, виды, каналы утечки и искажения информации. Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и доступности информации. Информационная безопасность в условиях функционирования в России глобальных сетей.

Тема 4. Методы и средства обеспечения информационной безопасности информационных систем

Общая проблема информационной безопасности информационных систем. Защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение). Защита информации от несанкционированного доступа. Компьютерные средства реализации защиты в информационных системах.

Тема 5. Использование защищенных компьютерных систем.

Политика безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных систем. Использование защищенных компьютерных систем. Примеры практической реализации.

Тема 6. Защита от разрушающих программных воздействий.

Понятие разрушающего программного воздействия. Методы перехвата и навязывания информации. Компьютерные вирусы. Понятия о видах вирусов. Современные антивирусные программы.

Тема 7 Особенности защиты в операционных системах.

Подходы к построению защищенной операционной системы. Административные меры защиты. Стандарты защищенности операционных систем. Виды уязвимости и атак на ОС. Классификация угроз безопасности операционной системы. Типичные атаки на операционную систему.

Тема 8. Особенности защиты информации в компьютерных сетях.

Классификация способов несанкционированного доступа и жизненный цикл атак. Нападения на политику безопасности и процедуры административного управления. Нападения на постоянные и сменные компоненты системы защиты. Нападения на протоколы информационного взаимодействия. Нападения на функциональные элементы компьютерных сетей.

Способы противодействия несанкционированному сетевому и межсетевому доступу. Аутентификация пользователя локальной сети. Разграничение доступа к локальной сети. Противодействие несанкционированному межсетевому доступу. Использование межсетевых экранов (Firewall). Критерии их оценки.

Защита виртуальных потоков на различных сетевых уровнях. Защита удаленного доступа к локальной сети. Безопасная доставка E-mail сообщений. Использование ключей и цифровых подписей. Сертификация серверов Интернет. Безопасность работы в Интернет с использованием браузера.

Тема 9. Защита программ и данных

Защита офисных документов. Способы распространения программного обеспечения. Техническая защита от несанкционированного копирования. Базовые методы нейтрализации систем защиты от несанкционированного копирования. Идентификация параметров персонального компьютера. Идентификация жестких дисков. Идентификация гибких дисков. Оценка уникальности конфигурации компьютера.

4. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ ДИСЦИПЛИНЫ

практические задания , в том числе в форме практической подготовки

Тема 1. Введение в проблему информационной безопасности.

Информационная безопасность: подходы и перспективы развития. Антивирусные программные комплексы. Восстановление зараженных файлов. Профилактика проникновения вредоносных программ.

Тема 2. Правовые и организационные аспекты защиты информации.

Необходимость защиты информации. Правовая защита: миф и реальность. Организационное устройство защиты информации.

Тема 3. Угрозы информационной безопасности и методы их реализации.

Угрозы безопасности информации и их виды. Современные методы реализации обнаружения угроз.

Тема 4. Методы и средства обеспечения информационной безопасности информационных систем

Использование антивирусных программ Защита документов MS WORD Защита книг MS EXCEL. Симметричные алгоритмы шифрования. Настройка защищенного сетевого соединения.

Тема 5. Использование защищенных компьютерных систем.

Компьютерные системы. Защита компьютерных систем.

5.МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Студенту важно уяснить технологию освоения учебного материала. Данные методические рекомендации позволят понять, как правильно организовать свое учебное время, научиться использовать различные формы обучения для оптимального овладения знаниями по предмету.

Для успешного освоения дисциплины, студент должен посещать все виды аудиторных занятий, вести конспекты лекционных и практических занятий; своевременно готовиться к аудиторным занятиям, используя соответствующие методические материалы, учебную и исследовательскую литературу и собственные конспекты; выполнять предусмотренные учебным планом виды работ, домашние задания на основе соответствующих методических материалов, а при возникновении вопросов обращаться к преподавателю за консультацией.

К числу используемых средств при освоении дисциплины относятся: рефераты, доклады, тесты.

Предполагается, что студенты должны самостоятельно дорабатывать учебный материал, рассмотренный в лекционном порядке. Для этого рекомендуется разделить тетрадь для конспекта лекций на три части. 2/3 листа использовать для фиксации лекции преподавателя, а на оставшейся части делать выписки-дополнения по теме из рекомендованной учебной и исследовательской литературы, правовых актов; вносить информацию, не затронутую в лекции. Такого рода «усовершенствованные» конспекты лекций позволят студенту не только повторить материал, рассмотренный в лекционном порядке, но вдумчиво изучить учебный и дополнительный материал, и, следовательно, получить более качественные знания.

Одной из наиболее эффективной форм обучения являются практические занятия. Основу работы составляет самостоятельное изучение студентами по заданию преподавателя отдельных вопросов, проблем, тем с последующим оформлением материала в виде доклада, сообщения и их совместное обсуждение.

Они представляют собой не только способ закрепить и углубить лекционный материал, но и осуществить контроль над ходом самостоятельной работы обучающихся. Форма практического занятия представляет собой синтез аудиторной и внеаудиторной работы. Студенты в течение учебной недели самостоятельно рассматривают вопросы по теме практического занятия. Аудиторная работа в форме практического занятия предусматривает решение задач, решение проблемной ситуации, выступление студента в качестве основного докладчика по отдельному вопросу в рамках индивидуального творческого занятия (реферата).

Практические занятия являются действенной формой приобщения студентов к использованию источников и исследовательской литературы на научной основе. Чаще всего используется либо вопросно-ответная форма, либо обсуждение рефератов, работа в малых группах, проведение ролевых игр и т.д.

Подготовка к практическим занятиям основана на плане, определенном преподавателем к каждой теме. Каждая тема практических занятий сопровождается перечнем нормативных правовых актов, а также учебной и исследовательской литературы.

Процесс подготовки к практическому занятию включает знакомство с соответствующей темой в учебнике, изучение исследовательской литературы.

При подготовке к практическим занятиям следует вести конспекты, которые представляют собой развернутый план ответа на вопрос, но не исчерпывающий ответ.

Таким конспектом, а также нормативным материалом студент вправе пользоваться во время ответа на занятии. В то же время, следует заметить, что студент не должен зачитывать конспект ответа. Он может лишь опираться на него, чтобы не потерять нить рассуждения.

Для ведения конспектов практических занятий следует завести отдельную тетрадь. Преподаватель периодически проверяет качество подготовки к практическим занятиям, собирая конспекты. Если студент пропустил практическое занятие, то он обязан явиться на консультацию к преподавателю, предъявить свой конспект по пропущенной теме и отчитаться в устной форме.

Цель каждого студента - проявить свои знания во время проведения практических занятий. При этом могут использоваться самые разнообразные формы работы: выступление в качестве основного докладчика, выступление с рефератом, участие в дискуссиях и круглых столах, др. Это придает учебному занятию характер коллективной работы, повышает внимание и интерес студентов.

Выступление на практическом занятии носит, преимущественно, добровольный характер. Студент, желающий ответить на вопрос плана, занимает место за кафедрой и выполняет функцию основного докладчика. Его речь не может прерываться, либо комментироваться. После окончания выступления студенты группы вправе задать докладчику вопросы уточняющего характера, либо обратить внимание на слабо освещенные аспекты темы. При этом преподаватель оценивает «качество» вопросов. Они не должны дублировать озвученный материал, содержать однозначных ответов (да – нет), должны быть корректно сформулированы и соответствовать вопросу плана. Если внимание учебной группы во время выступления основного докладчика рассеяно, то преподаватель предоставляет ему самому право сформулировать ряд вопросов, и адресует их конкретным студентам. При необходимости преподаватель задает вопросы докладчику, либо студентам.

Аспекты, не освещенные основным докладчиком, рассматриваются в качестве дополнений к ответу. После этого группа переходит к рассмотрению следующего вопроса.

Практическое занятие завершается подведением итогов работы. Преподаватель резюмирует рассмотренные аспекты темы, отвечает на вопросы студентов, анализирует работу всей учебной группы и отдельных студентов.

Предусматривается, что обучающиеся должны самостоятельно дорабатывать учебный материал, рассмотренный в лекционном порядке.

Если возникают сложности с восприятием учебного материала, студенту следует обратиться к преподавателю. Для индивидуальной работы предусмотрены еженедельные

консультационные дни. День недели, время проведения консультаций указаны на стендах вуза по направлениям подготовки.

Наряду с аудиторной работой для студента при изучении дисциплины особое значение имеет самостоятельная работа в соответствии с предусмотренным учебным планом распределением времени. Методические рекомендации по осуществлению самостоятельной работы представлены в разделе «Учебно-методическое обеспечение самостоятельной работы обучающихся».

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Самостоятельная работа обучающихся проводится в виде самостоятельной подготовки во внеурочное время путем работы с рекомендуемой литературой, нормативными актами, периодикой. Самостоятельная работа обучающихся проводится в виде самостоятельной подготовки во внеурочное время путем работы с рекомендуемой литературой, нормативными актами, периодикой.

Самостоятельная работа студентов очной формы обучения предполагает подготовку теоретического материала для опроса на практических занятиях и вопросов для самостоятельного изучения, решение тестов, варианты которой представлены ниже.

Для самопроверки качества усвоения учебного материала предусмотрены тестовые задания. Обучающиеся самостоятельно могут решать их, тем самым, готовясь к итоговому тестированию.

Если возникают сложности с восприятием учебного материала, студентам следует обратиться к преподавателю.

Методические рекомендации по написанию рефератов, докладов

Реферат (от lat. «докладывать», «сообщать») представляет собой письменный доклад на определенную тему, включающий обзор соответствующих литературных и других источников, а также собственные выводы по основным вопросам данной темы. Реферат является первой ступенью на пути освоения навыков проведения научно-исследовательской работы. Избранная студентом проблема изучается и анализируется на основе одного или нескольких источников, реферат направлен на анализ одной или нескольких научных работ.

Написание реферата, доклада не является обязательной работой обучающегося и практикуется в учебном процессе в целях приобретения студентом необходимой профессиональной подготовки, развития умения и навыков самостоятельного научного поиска: изучения литературы по выбранной теме, анализа различных источников и точек

зрения, обобщения материала, выделения главного, формулирования выводов и т.п. С помощью рефератов студент глубже постигает наиболее сложные проблемы дисциплины, учится лаконично излагать свои мысли, правильно оформлять работу, докладывать результаты своего труда.

Целями написания реферата, доклада являются:

- развитие у студентов навыков поиска актуальных проблем современного законодательства;
- развитие навыков краткого изложения материала с выделением лишь самых существенных моментов, необходимых для раскрытия сути проблемы;
- развитие навыков анализа изученного материала и формулирования собственных выводов по выбранному вопросу в письменной форме, научным, грамотным языком.

Задачами написания реферата, доклада являются:

- обучение студента максимально верно передать мнения авторов, на основе работ которых обучающийся пишет свой реферат;
- обучение студента грамотно излагать свою позицию по анализируемой в реферате проблеме;
- подготовка студента к дальнейшему участию в научно – практических конференциях, семинарах и конкурсах;
- помощь студенту определиться с интересующей его темой, дальнейшее раскрытие которой возможно осуществить при написании курсовой работы или выпускной квалификационной работы;
- выработка навыков изложения причины своего согласия (несогласия) с мнением того или иного автора по данной проблеме.

Процесс написания реферата, доклада включает:

- выбор темы;
- составление плана;
- подбор источников и их изучение;
- написание текста работы и ее оформление.

Тему реферата, доклада студент выбирает самостоятельно, опираясь на предлагаемую тематику. В работе на основе тщательного анализа и обобщения научного материала сопоставляются различные взгляды авторов и определяется собственная позиция обучающегося с изложением соответствующих аргументов.

Работу над рефератом, докладом следует начинать с общего ознакомления с темой (прочтение соответствующего раздела учебника, учебного пособия и других источников). Однако перечень источников не должен связывать инициативу обучающегося. Он может

использовать научную литературу, подобранную самостоятельно. Особенно внимательно необходимо следить за новой литературой по избранной проблематике, в том числе за журнальными статьями. Кроме того, не лишним будет ознакомиться с рефератами предшественников по аналогичной или похожей теме, где можно почерпнуть некоторые идеи (при этом обязательно сделать сноску в тексте работы), а также принять во внимание правила оформления реферата, доклада. В процессе изучения литературы рекомендуется делать выписки, постепенно группируя и накапливая теоретический и практический материал. План реферата, доклада должен быть составлен таким образом, чтобы он раскрывал тему работы.

Структурными элементами реферата, доклада являются: титульный лист, содержание, введение, основная часть, заключение, список литературы, приложения.

Во «введении» необходимо рассмотреть актуальность темы с точки зрения современной науки, нынешнего состояния общества и культуры. Следует указать место обозначенной проблемы среди других, как частных, так и более общих, а также избранное Вами направление ее рассмотрения.

Введение оканчивается формулированием цели и задач исследования. Цель реферата может заключаться в том, чтобы обобщить или сравнить различные подходы к рассмотрению проблемы, выявить наименее или наиболее изученные ее стороны, показать основной смысл исследовательского направления, наметить пути его дальнейшего развития. Задачи (их может быть несколько) отражают более детальное рассмотрение цели. В качестве задач могут выступать: анализ литературы по избранной теме, сравнение различных подходов к решению проблемы, исторический обзор, описание основных понятий исследования и т.д.

«Основная часть» посвящена самому исследованию. В ней, в соответствии с поставленными задачами, раскрывается тема работы. Здесь нужно проследить пути решения поставленной проблемы. Это делается с помощью цитирования и пересказа текста используемых вами литературных источников. Собственные слова, как правило, здесь нужны для смысловых связей и для высказывания своего отношения к позиции автора.

При подготовке реферата, доклада важно научиться выделять главное в текстах первоисточников, с которыми Вы работаете. Прежде всего, надо «понять» название монографии или статьи, потому что именно в нем, как правило, концентрируется основная идея автора. Затем посмотреть оглавление и предметный указатель (чтобы понять, есть ли в книге то, что вам нужно). Потом следует найти те части текста, которые содержат

ключевые положения изучаемой научной проблемы, причем изложить не только выводы авторов, но и те исследования, которые к ним привели.

Для написания основной части требуется особенно тщательно выделять из прочитанных научных текстов главные положения, относящиеся к проблеме, а затем кратко, логично и литературно грамотно их излагать. С этой целью полезно идти от общего к частному: название и ключевые понятия теории, ее автор, когда была предложена и почему, к каким результатам привела, кем и как критиковалась, кто дополнял и развивал ее, каково современное состояние проблемы, мнение автора по этой проблеме.

Основная часть может представлять собой цельный текст, а может состоять из нескольких параграфов, начинающихся пронумерованным подзаголовками. Для иллюстрации основного содержания можно использовать рисунки, схемы, графики, таблицы, диаграммы и прочие наглядные материалы.

Выводы завершают основную часть. В них кратко излагаются основные результаты работы по пунктам, соответствующим задачам исследования и отражается мнение автора о результатах сравнения и/или обобщения точек зрения различных ученых. В выводах должно быть показано, что цель исследования достигнута.

«Заключение» представляет собой общий итог работы с кратким перечислением выполненных автором этапов исследования. Здесь же можно отметить пути дальнейшего исследования, возможности практического применения полученных результатов и т.д.

Изложение материала должно быть кратким, точным, последовательным. Необходимо избегать непривычных или двусмысленных понятий и категорий, сложных грамматических оборотов. Термины, отдельные слова и словосочетания допускается заменять принятыми текстовыми сокращениями, смысл которых ясен из контекста. Рекомендуется включать в реферат схемы и таблицы, если они помогают раскрыть основное содержание проблемы и сокращают объем работы.

Оформление реферата, доклада

Объем реферата обычно содержит 18 ± 3 страниц печатного текста. Количество страниц зависит от объективной сложности раскрытия темы и доступности литературных источников.

Первый лист реферата, доклада - титульный (на титульном листе номер страницы не ставится, хотя и учитывается).

Список литературы не должен ограничиваться только учебниками и не может быть менее 5 источников. Список литературы должен содержать названия источников,

фамилии и инициалы их авторов, издательство, место и год опубликования, а также общее количество страниц. Библиография выстраивается в алфавитном порядке.

В процессе работы необходимо делать ссылки на работы ученых, мысли которых использованы в работе, и по мере надобности оформлять сноски.

| | |
|---------------------------------|-------------------------------------|
| Наименование | Формат |
| Формат бумаги | A4 |
| Шрифт | Times New Roman, размер (кегель) 14 |
| Междустрочный интервал | 1,5 |
| Поля: слева/справа/сверху/снизу | 3/1,5/2/2 |
| Сноски (шрифт) | Times New Roman, размер 10 |
| Номер страницы | |

Реферат, доклад студент может иллюстрировать презентацией. При составлении презентации необходимо учитывать следующие требования.

Для подготовки презентации рекомендуется использование программы Microsoft PowerPoint. Сформулировать цель презентации, определиться с форматом, выстроить логическую цепочку, определиться с картинками иллюстраций, диаграммам

- презентация не должна быть меньше 10 слайдов;
- первый лист – это титульный лист, на котором обязательно должны быть представлены: название проекта; фамилия, имя, отчество автора;
- следующим слайдом должно быть содержание, где представлены основные этапы (моменты) презентации; желательно, чтобы из содержания по гиперссылке можно перейти на необходимую страницу и вернуться вновь на содержание;
- дизайн-эргономические требования: сочетаемость цветов, ограниченное количество объектов на слайде, цвет текста;
- последними слайдами презентации должны быть глоссарий и список литературы.

Качественное освоение учебного материала невозможно без освоения соответствующего понятийного аппарата, с этой целью студенты могут воспользоваться глоссарием, включающим термины и понятия. Термин – это слово, или сочетание слов, являющееся точным обозначением определенного понятия какой-либо специальной области науки. Понятие – мысль о предметах и явлениях действительности, отображающая их общие и существенные признаки, связи и отношения.

План-график выполнения самостоятельной работы

| № п/ | Учебно-образовательные единицы дисциплины | Трудоемкость | Виды самостоятельной | Часы |
|------|---|--------------|----------------------|------|
|------|---|--------------|----------------------|------|

| п | | СРС, часы | работы студентов | Очная Очно- заочная | заочная |
|---|--|--------------|------------------------------------|---------------------------|---------|
| 1 | Тема 1. Введение в проблему информационной безопасности. Тема 3. Угрозы информационной безопасности и методы их реализации. | | подготовка к практическому занятию | 2 | 2 |
| | | | Реферат, доклад, тест | 4 | 7 |
| 2 | Тема 4. Методы и средства обеспечения информационной безопасности информационных систем Тема 5. Использование защищенных компьютерных систем. Тема 6. Защита от разрушающих программных воздействий. | | подготовка к практическому занятию | 2 | - |
| | | | Реферат, доклад, тест | 4 | 9 |
| 3 | Тема 7 Особенности защиты в операционных системах. Тема 8 Особенности защиты информации в компьютерных сетях. Тема 9. Защита программ и данных | | подготовка к практическому занятию | - | - |
| | | | Реферат, доклад, тест | 4 | 10 |
| | | | Подготовка к зачету | 2 | 2 |

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет самостоятельная индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), то есть дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

Учебно – методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

| | | |
|--------------------------------------|-------------------------------------|---|
| для лиц с нарушениями зрения: | для лиц с нарушениями слуха: | для лиц с нарушениями опорно – двигательного аппарата: |
|--------------------------------------|-------------------------------------|---|

| | | |
|---|--|---|
| <ul style="list-style-type: none"> - в печатной форме увеличенный шрифтом; - в форме электронного документа; - в форме аудиофайла. | <ul style="list-style-type: none"> - в печатной форме; - в форме электронного документа; | <ul style="list-style-type: none"> - в печатной форме увеличенный шрифтом; - в форме электронного документа; - в форме аудиофайла. |
|---|--|---|

7. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В учебном процессе используются лицензионные версии программных продуктов, обеспечивающие повышение качества проведения занятий на основе использования современной компьютерной техники: операционная система Windows XP, 7, 8.1; пакет программ Microsoft Office 2013; антивирусное программное обеспечение eset ENDPOINT ANTIVIRUS. Электронно-библиотечная система (ЭБС) www.znanium.com. Презентации оформляются в программе PowerPoint

В случае возникновения (возобновления) сложной эпидемиологической обстановкой в регионе, вызванной пандемией коронавируса COVID-19 или иными неблагоприятными условиями, учебный процесс проводится в дистанционной форме с применением ДОТ посредством платформы для проведения аудио и видеоконференций Zoom в режиме двусторонней видеоконференции, где обучающийся и преподаватель имеют возможность видеть и слышать друг друга, согласно следующей процедуре:

- профессорско-преподавательский состав осуществляет занятия с обучающимися, текущую и промежуточную аттестацию с применением ДОТ, включая обучение с использованием современных информационных и телекоммуникационных систем, методическое, технологическое и организационное обеспечение учебного процесса; оказывает обучающимся индивидуальные консультации с применением информационных и телекоммуникационных технологий посредством: электронной почты; онлайн консультации с использованием телекоммуникационных технологий (программа Zoom); консультации с использованием электронной информационно-образовательной среды (чат, вебинар), консультации в форумах учебных дисциплин электронной системы дистанционного обучения;

- каждый обучающийся имеет свободный доступ ко всем сервисам ЭИОС, который персонализирован (под единой учетной записью) и имеет единую точку входа;

- лицо, ответственное за техническое сопровождение учебного процесса, осуществляет подключение к вебинарной комнате преподавателя, для обеспечения участия обучающихся, в изучении учебных дисциплин.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для обеспечения подготовки обучающихся по направлению 40.03.01 «Юриспруденция» в «Дальневосточном филиале Федерального государственного бюджетного образовательного учреждения высшего образования «Всероссийская академия внешней торговли Министерства экономического развития Российской Федерации»» создана необходимая информационная база, и обеспечен доступ обучающихся к различным сетевым источникам информации, включая Интернет, что способствует эффективному получению профессиональных навыков.

Освоение дисциплины осуществляется в учебной аудитории № 206 «Компьютерный класс», рассчитанной на 25-30 студентов, оборудованной мультимедийным комплексом и экраном для демонстрации слайдовых презентаций и иных необходимых материалов. Для самостоятельной работы обучающихся могут быть использованы учебные аудитории № 415 («Научно-исследовательская лаборатория»), № 202 («Типография»), № 206 («Компьютерный класс»).

Аудитории библиотеки 207, 209 оборудованные 5 рабочими станциями с доступом к сети «Интернет» и в электронную информационно-образовательную среду организации, и комплектом учебной мебели на 35 посадочных мест.

В соответствии с содержанием теоретической и практической части курса используется научная литература, электронные ресурсы, техническое оборудование (офисная техника, компьютеры) ДВФ ВАВТ и тех организаций и учреждений, где студенты проходят исследования и производственную практику ,в том числе:

1. учебники, учебно – методические пособия;
2. технические средства обучения (компьютерная техника, аудио – и видеоаппаратура);
3. проектор и ноутбук;
4. учебно – наглядные пособия (стенды, плакаты).

Стенды:

1. Правила записи имени файла.
2. Элементы окна Windows.
3. Файлы операционной системы.
4. Команды операционной системы.
5. Управление панелями.
6. Вывод информации о файлах.
7. Технические средства компьютерных информационных технологий.
8. Правила работы за персональным компьютером.

Обучение инвалидов и лиц с ограниченными возможностями здоровья осуществляется с применением специального оборудования:

а) для лиц с нарушением слуха (акустический усилитель и колонки, мультимедийный проектор); б) для лиц с нарушением зрения (мультимедийный проектор (использование презентаций с укрупненным текстом); в) для лиц с нарушением опорно-двигательного аппарата (персональные мобильные компьютеры-нетбуки).

При необходимости используется Каб. № 107 – «Кабинет для лиц с ОВЗ».

9. БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Основная литература:

ЭЛЕКТРОННО – БИБЛИОТЕЧНОЙ СИСТЕМЫ (ЭБС)

адрес: [www. znanium.com](http://www.znanium.com)

Информационная безопасность : практикум / С. В. Озёрский, И. В. Попов, М. Е. Рычаго, Н. И. Улендеева. - Самара : Самарский юридический институт ФСИН России, 2019. - 84 с. - ISBN 978-5-91612-276-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1094244>

Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: <https://doi.org/10.29039/1761-6>. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1189326>

Имеются в наличии в электронных библиотечных системах в виде электронного документа для освоения дисциплины инвалидами или лицами с ограниченными возможностями здоровья.

Дополнительная литература:

ЭЛЕКТРОННО – БИБЛИОТЕЧНОЙ СИСТЕМЫ (ЭБС)

адрес: [www. znanium.com](http://www.znanium.com)

Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учеб. пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2019. — 223 с. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/textbook_5cc15bb22f5345.11209330. - ISBN 978-5-16-014397-2. - Текст : электронный. - URL: <https://znanium.com/catalog/product/979415>

Анализ состояния защиты данных в информационных системах / Денисов В.В. - Новосибирск : НГТУ, 2012. - 52 с.: ISBN 978-5-7782-1969-4. - Текст : электронный. - URL: <https://znanium.com/catalog/product/546005>

Имеются в наличии в электронных библиотечных системах в виде электронного документа для освоения дисциплины инвалидами или лицами с ограниченными возможностями здоровья.

Профессиональные базы данных и информационные поисковые системы, интернет-ресурсы свободного доступа

1. Базы данных международных индексов научного цитирования Scopus <https://www.scopus.com/search/form.uri?display=basic#basic>
2. Портал открытых данных России <https://data.gov.ru/>
3. ИД «Connect» - отраслевой информационно-аналитический портал в сфере информационных технологий <https://www.connect-wit.ru/>
4. «Компьютерра» – журнал о современных информационных технологиях <https://www.computerra.ru/>
5. «Информационные технологии» - журнал <http://novtex.ru/IT/index.htm>
- «Компьютер-пресс» - журнал <https://compress.ru/>
6. <http://pravo.gov.ru/> - Официальный интернет-портал правовой информации:
7. <http://government.ru/> - Интернет-портал Правительства Российской Федерации:
 - <http://government.ru/rugovclassifier/> - деятельность;
8. <https://www.vsrfr.ru/> - Официальный сайт Верховного Суда Российской Федерации:
 - <https://vsrf.ru/documents/practice/?year=2021> – обзоры судебной практики;
9. <http://pravo.minjust.ru/> - Нормативные правовые акты в Российской Федерации (Министерство юстиции Российской Федерации):
10. <https://www.dissercat.com/> - Научная электронная библиотека диссертаций и авторефератов
11. <https://minjust.gov.ru/ru/> - сайт Министерства юстиции Российской Федерации
 - <https://minjust.gov.ru/ru/documents/> - документы;
 - <https://minjust.gov.ru/ru/pages/pravovaya-informaciya/> - правовая информация.
12. <https://kamgov.ru/> - Официальный сайт Камчатского края:
 - <https://www.kamgov.ru/gov-entity/iogv> - исполнительные органы;
 - <https://www.kamgov.ru/gosudarstvennaya-sluzhba> - государственная служба
13. <https://gossluzhba.gov.ru/> - Федеральный портал государственной службы и управленческих кадров:

- <http://www.jur-words.info/> - Юридический словарь
- 14. Официальный сайт Федеральной службы по техническому и экспортному контролю
<https://fstec.ru/>
- 15. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. <https://digital.gov.ru/ru/ministry/common/>
- 16. Министерство иностранных дел
(Международная информационная безопасность) <https://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost>
- 17. Информационно-технологический центр Камчатского края <https://itc.kamgov.ru/>
- 18. Министерство цифрового развития Камчатского края
<https://www.kamgov.ru/digital>
- 19. СПС Консультант Плюс <http://www.consultant.ru/>



Дальневосточный филиал Федерального государственного бюджетного
образовательного учреждения высшего образования
«Всероссийская академия внешней торговли
Министерства экономического развития Российской Федерации»

КАФЕДРА «ЕСТЕСТВЕННЫЕ И СОЦИАЛЬНО – ГУМАНИТАРНЫЕ НАУКИ»

ОЦЕНОЧНЫЕ СРЕДСТВА
по дисциплине «Информационная безопасность, защита персональных
данных»
40.03.01 «Юриспруденция»
профиль «Гражданско-правовой»
Форма подготовки (очная/заочная/очно-заочная)

г. Петропавловск-Камчатский
2020

10.1 ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

| № п/п | Контролируемые компетенции | Оценочные средства |
|----------|----------------------------|--|
| 1,2,3,4 | ОК-4, ОК-3, ОПК-2, ПК-11 | Устный ответ, доклад, реферат, тест, контрольные вопросы, выносимые на зачет |

Для студентов с ограниченными возможностями здоровья предусмотрены следующие оценочные средства:

| № п/п | Категории студентов | Виды оценочных средств | Форма контроля и оценки результатов обучения |
|----------|--|-------------------------------------|--|
| 1 | С нарушением слуха | Письменные работы, вопросы к зачету | Преимущественно письменная проверка |
| 2 | С нарушением зрения | Собеседование по вопросам к зачету | Преимущественно устная проверка |
| 3 | С нарушением опорно – двигательного аппарата | Собеседование по вопросам к зачету | Организация взаимодействия с обучающимися посредством электронной почты, письменная проверка |

10.2 План – график проведения контрольно-оценочных мероприятий

| Название оценочного мероприятия | Вид оценочного средства | Объект контроля | Срок (сем/ курс.) Очное/очно- заочное/заочное |
|---------------------------------|----------------------------------|---|--|
| <i>Входной контроль</i> | <i>Устный ответ</i> | <i>ответы</i> | 6/6/3 |
| <i>Текущий контроль</i> | <i>Доклад, реферат, тест</i> | <i>Качество освоения материала</i> | 6/6/3 |
| <i>Выходной контроль</i> | <i>Собеседование по вопросам</i> | <i>Правильность ответов на поставленные вопросы</i> | 6/6/3 |

10.3 Контрольные вопросы, выносимые на зачет

1. Информационная безопасность. Предмет и объект защиты.
2. Угроза безопасности. Уязвимость системы. Атака.
3. Несанкционированный доступ. Виды угроз.
4. Компьютерные вирусы и черви.
5. Макровирусы.
6. Полиморфные вирусы.
7. Троянские кони (закладки).
8. Антивирусы и "антитроянцы".
9. Антивирусные программы в Интернете.

10. Межсетевые экраны. Опыт работы с межсетевым экраном.
11. Политика безопасности.
12. Назначение и функции межсетевых экранов.
13. Виртуальные частные сети.
14. Уязвимость компьютера и сети. Виды угроз.
15. Угроза отказ в обслуживании.
16. Социальная инженерия и ИБ.
17. Генераторы вирусов.
18. Законодательная база РФ в области информационной безопасности.
19. Отражение проблем ИБ в Интернете.
20. Парольная защита.
21. Программы слежения за работой пользователя (клавиатурные шпионы).
22. Системы обнаружения уязвимостей (сетевые сканеры).
23. Обнаружение атак.
24. Защита информации в базах данных.
25. Анализаторы протоколов (снифферы).
26. Мандатный и дискреционный доступ.
27. Шифрование. Метод подстановки.
28. Матрицы Вижинера.
29. Частотный анализ текстов.
30. Шифрование методом перестановки.
31. Генераторы случайных чисел.
32. Криптосистема с открытым ключом

10.4. Темы докладов, рефератов

1. Методы борьбы с фишинговыми атаками.
2. Законодательство о персональных данных.
3. Защита авторских прав.
4. Назначение, функции и типы систем видеозащиты.
5. Как подписывать с помощью ЭЦП электронные документы различных форматов.
6. Обзор угроз и технологий защиты Wi-Fi-сетей.
7. Проблемы внедрения дискового шифрования.
8. Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.
9. Особенности процессов аутентификации в корпоративной среде.
10. Квантовая криптография.
11. Утечки информации: как избежать. Безопасность смартфонов.

- 12.Безопасность применения пластиковых карт - законодательство и практика.
- 13.Защита CD- и DVD-дисков от копирования.
- 14.Современные угрозы и защита электронной почты.
- 15.Программные средства анализа локальных сетей на предмет уязвимостей.
- 16.Безопасность применения платежных систем - законодательство и практика.
- 17.Аудит программного кода по требованиям безопасности.
- 18.Антишпионское ПО (antispware).
- 19.Обеспечение безопасности Web-сервисов.
- 20.Защита от внутренних угроз.
- 21.Технологии RFID.
- 22.Уничтожение информации на магнитных носителях.
- 23.Ботнеты - плацдарм современных кибератак.
- 24.Цифровые водяные знаки в изображениях.
- 25.Электронный документооборот. Модели нарушителя.
- 26.Идентификация по голосу. Скрытые возможности.
- 27.Безопасность океанских портов.
- 28.Безопасность связи.
- 29.Безопасность розничной торговли.
- 30.Банковская безопасность.
- 31.Информатизация управления транспортной безопасностью.
- 32.Биопаспорт.
- 33.Обзор современных платформ архивации данных.
- 34.Что такое консалтинг в области ИБ.
- 35.Бухгалтерская отчетность как источник рассекречивания информации.
- 36.Управление рисками: обзор употребительных подходов.
- 37.Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности.
- 38.Распределенные атаки на распределенные системы.
- 39.Оценка безопасности автоматизированных систем.
- 40.Windows и Linux: что безопаснее?
- 41.Функциональная безопасность программных средств.
- 42.Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств.
- 43.Информационная безопасность: экономические аспекты.

10.5 Тестовые задания

Выбишите правильные ответы.

1. **Возможность получения информации и ее использования это:**
 - сохранение информации
 - распространение информации
 - предоставление информации
 - конфиденциальность информации
 - доступ к информации
2. **Информация, переданная или полученная пользователем информационно-телекоммуникационной сети:**
 - электронное сообщение
 - информационное сообщение
 - текстовое сообщение
 - визуальное сообщение
 - sms-сообщение
3. **Все компоненты информационной системы предприятия, в котором накапливаются и обрабатываются персональные данные это:**
 - информационная система персональных данных
 - база данных
 - централизованное хранилище данных
 - система статэксpress
 - сервер
4. **Действия с персональными данными (согласно закону), включая сбор, систематизацию, накопление, хранение, использование, распространение и т. д. это:**
 - «исправление персональных данных»
 - «работа с персональными данными»
 - «преобразование персональных данных»
 - «обработка персональных данных»
 - «изменение персональных данных»
5. **Действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных:**
 - выделение персональных данных
 - обеспечение безопасности персональных данных
 - деаутентификация
 - деавторизация
 - деперсонификация

6. По режиму обработки персональных данных в информационной системе информационные системы подразделяются на:

- многопользовательские
- однопользовательские
- без разграничения прав доступа
- с разграничением прав доступа
- системы, не имеющие подключений

7. Процесс сообщения субъектом своего имени или номера, с целью получения определённых полномочий (прав доступа) на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом:

- авторизация
- аутентификация
- обезличивание
- деперсонализация
- идентификация

9. Процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации:

- авторизация
- обезличивание
- деперсонализация
- аутентификация
- идентификация

10. Процесс, а также результат процесса проверки некоторых обязательных параметров пользователя и, при успешности, предоставление ему определённых полномочий на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом

- авторизация
- идентификация
- аутентификация
- обезличивание
- деперсонализация

11. Простейшим способом идентификации в компьютерной системе является ввод идентификатора пользователя, который имеет следующее название:

- токен

password

пароль

login

смарт-карта

12. Основное средство, обеспечивающее конфиденциальность информации, посылаемой по открытым каналам передачи данных, в том числе – по сети интернет:

идентификация

аутентификация

авторизация

экспертиза

шифрование

13. Для безопасной передачи данных по каналам интернет используется технология:

www

dicom

vpn

ftp

xml

14. Комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами и защищающий компьютерные сети от несанкционированного доступа:

антивирус

замок

брандмауэр

криптография

экспертная система

15. За правонарушения в сфере информации, информационных технологий и защиты информации данный вид наказания на сегодняшний день не предусмотрен:

дисциплинарные взыскания

административный штраф

уголовная ответственность

лишение свободы

смертная казнь

несанкционированный доступ к информации это:

16. Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально

работа на чужом компьютере без разрешения его владельца

вход на компьютер с использованием данных другого пользователя

доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей

доступ к субд под запрещенным именем пользователя

17. «Персональные данные» это:

любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу

фамилия, имя, отчество физического лица

год, месяц, дата и место рождения, адрес физического лица

адрес проживания физического лица

сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»

18. В данном случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности:

выход в интернет без разрешения администратора

при установке компьютерных игр

в случаях установки нелицензионного ПО

в случае не выхода из информационной системы

в любом случае неправомерного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности

19. Может ли сотрудник быть привлечен к уголовной ответственности за нарушения правил информационной безопасности предприятия:

нет, только к административной ответственности

нет, если это государственное предприятие

да

да, но только в случае, если действия сотрудника нанесли непоправимый вред

да, но только в случае осознанных неправомерных действий сотрудника

20. Процедура, проверяющая, имеет ли пользователь с предъявленным идентификатором право на доступ к ресурсу это:

идентификация

аутентификация
стратификация
регистрация
авторизация

21. Наиболее опасным источником угроз информационной безопасности предприятия являются:

другие предприятия (конкуренты)
сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам
рядовые сотрудники предприятия
возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных
хакеры

22. Выберите, можно ли в служебных целях использовать электронный адрес (почтовый ящик), зарегистрированный на общедоступном почтовом сервере, например на mail.ru:

нет, не при каких обстоятельствах
нет, но для отправки срочных и особо важных писем можно
можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера
можно, если информацию предварительно заархивировать с помощью программы Winrar с паролем
можно, если других способов электронной передачи данных на предприятии или у пользователя в настоящий момент нет, а информацию нужно переслать срочно

23. Документированная информация, доступ к которой ограничивает в соответствии с законодательством РФ:

информация составляющая государственную тайну
информация составляющая коммерческую тайну
персональная
конфиденциальная информация
документированная информация

24. Для того чтобы снизить вероятность утраты информации необходимо:

регулярно производить антивирусную проверку компьютера
регулярно выполнять проверку жестких дисков компьютера на наличие ошибок

регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты)

защитить вход на компьютер к данным паролем

проводить периодическое обслуживание ПК

пароль пользователя должен

содержать цифры и буквы, знаки препинания и быть сложным для угадывания

содержать только цифры

содержать только буквы

иметь явную привязку к владельцу (его имя, дата рождения, номер телефона и т.п.)

быть простым и легко запоминаться, например «123», «111», «qwerty» и т.д.

25. Информационная безопасность обеспечивает...

блокирование информации

искажение информации

сохранность информации

утрату информации

подделку информации

26. Закон Российской Федерации «О государственной тайне» был принят в следующем году:

1982

1985

1988

1993

2005

27. Документированной информацией, доступ к которой ограничен в соответствии с законодательством РФ, называется:

конфиденциальная

персональная

документированная

информация составляющая государственную тайну

информация составляющая коммерческую тайну

28. В статье 272 уголовного кодекса говорится...

о неправомерном доступе к компьютерной информации

о создании, исполнении и распространении вредоносных программ для ЭВМ

о нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети

о преступлениях в сфере компьютерной информации

об ответственности за преступления в сфере компьютерной информации

28. Федеральный закон «Об информации, информатизации и защите информации»

направлен на:

регулирование взаимоотношений в информационной сфере совместно с гражданским кодексом РФ

регулирование взаимоотношений в гражданском обществе РФ

регулирование требований к работникам служб, работающих с информацией

формирование необходимых норм и правил работы с информацией

формирование необходимых норм и правил, связанных с защитой детей от информации

29. Хищение информации – это...

несанкционированное копирование информации

утрата информации

блокирование информации

искажение информации

продажа информации

30. Владелец информации первой категории является...

государство

коммерческая организация

муниципальное учреждение

любой гражданин

группа лиц, имеющих общее дело

31. Владелец информации второй категории является...

простые люди

государство

коммерческая организация

муниципальное учреждение

некоммерческая организация

32. Владелец информации третьей категории является...

люди

государство

муниципальное учреждение

учреждение

некоммерческая организация

33. Информацией, составляющей государственную тайну, владеют:

государство

только образовательные учреждения

только президиум верховного совета РФ

граждане российской федерации

только министерство здравоохранения

34. Информацией, составляющей коммерческую тайну, владеют:

государство

различные учреждения

государственная дума

граждане российской федерации

медико-социальные организации

35. Персональными данными владеют:

государство

различные учреждения

государственная дума

жители российской федерации

медико-социальные организации

36. Доступ к информации – это:

обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц

действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц

информация, переданная или полученная пользователем информационно-телекоммуникационной сети

возможность получения информации и ее использования

37. Документированная информация, доступ к которой ограничивается в соответствии с законодательством российской федерации это:

конфиденциальная информация

документы оферта и договоров

факс

личный дневник

законы РФ

38. Пластиковая карточка, содержащая чип для криптографических вычислений и встроенную защищенную память для хранения информации:

токен

password

пароль

login

смарт-карта

39. Устройство для идентификации пользователей, представляющее собой мобильное персональное устройство, напоминающие маленький пейджер, не подключаемые к компьютеру и имеющие собственный источник питания:

токен

автономный токен

usb-токен

устройство ibutton

смарт-карта

40. Доступ пользователя к информационным ресурсам компьютера и / или локальной вычислительной сети предприятия должен разрешаться только после:

включения компьютера

идентификации по логину и паролю

запроса паспортных данных

запроса доменного имени

запроса фео

40. Аппаратные модули доверенной загрузки «аккорд - амдз» представляют собой...

аппаратный контролер

электронный замок

система контроля

сетевой адаптер

копировальный аппарат

41. Электронные замки «соболь» предназначены для ...

обеспечения доверенной загрузки компьютера и контроля целостности файлов в системах

сканирования отпечатков пальцев
проверки скорости и загрузки файлов
общего контроля
идентификации пользователя
для защиты от злоумышленников необходимо использовать:
системное программное обеспечение
прикладное программное обеспечение
антивирусные программы
компьютерные игры
музыку, видеофильмы

42. Федеральный закон "Об информации, информатизации и защите информации" дает определение информации:

текст книги или письма
сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
сведения о явлениях и процессах
факты и идеи в формализованном виде
шифрованный текст, текст на неизвестном языке

43. Обеспечение информационной безопасности есть обеспечение...

Независимости информации
Изменения информации
Копирования информации
Сохранности информации
Преобразования информации

10.6 Критерии оценки знаний студентов

Критерии оценки знаний обучаемых при проведении тестирования.

Оценка «**отлично**» выставляется при условии правильного ответа студента не менее чем 85 % тестовых заданий.

Оценка «**хорошо**» выставляется при условии правильного ответа студента не менее чем 70 % тестовых заданий.

Оценка «**удовлетворительно**» выставляется при условии правильного ответа студента не менее 51 %.

Оценка «**неудовлетворительно**» выставляется при условии правильного ответа студента

менее чем на 50 % тестовых заданий.

Критерии оценки реферата, доклада

- оценка **«отлично»** выставляется за самостоятельно написанный реферат по теме; умение излагать материал грамотно и последовательно; аргументировать свою точку зрения, корректно ссылаясь на авторитетные источники; делать необходимые обобщения и выводы;
- оценка **«хорошо»** ставится, если реферат в основном удовлетворяет требованиям на оценку «отлично», но при этом имеет один из недостатков: в изложении допущены небольшие пробелы, недочеты, не искажившие содержание реферата; допущена ошибка или более двух недочетов при освещении второстепенных вопросов, которые легко исправляются по замечанию преподавателя. В реферате может быть недостаточно полно развернута аргументация;

оценка **«удовлетворительно»** ставится, если неполно или непоследовательно раскрыто основное содержание, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала; имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, которые были исправлены после замечаний преподавателя; студент не может применить теорию в новой ситуации;

оценка **«неудовлетворительно»** ставится, если не раскрыто основное содержание учебного материала; обнаружено незнание или непонимание большей или наиболее важной части учебного материала; допущены ошибки в определении понятий, при использовании терминологии, которые не были исправлены после нескольких замечаний преподавателя; нарушена логика в изложении материала, нет необходимых обобщений и выводов; недостаточно сформированы навыки письменной речи; реферат является плагиатом других рефератов более чем на 90%.

Критерии оценки итогового контроля

При оценке ответов студента в процессе итогового контроля оценивается:

- уверенные знания, умения и навыки, включенные в соответствующую компетенцию;
- знание ситуации и умение применить правильный научный методический подход и инструментарий для решения практических и лабораторных задач;
- умение выделять приоритетные направления в решении различного рода практических задач;
- способность устанавливать причинно-следственные связи в изложении материала,

делать выводы;

- умение применять теоретические знания для анализа конкретной социально-экономической ситуации.

Уровень знаний обучающихся определяется следующими оценками:

| | |
|------------------------------|---|
| Оценка « Зачтено » | Выставляется за глубокое знание предусмотренного программой материала, содержащегося в основных и дополнительных источниках литературы; логично выстроенный и лаконично представленный ответ на основной и дополнительные вопросы; умение анализировать изученные явления в их взаимосвязи с диалектическим развитием; за умение применять теоретические положения при решении практических задач. Компетенции, оцениваемые при ответе, сформированы полностью. |
| Оценка « Не зачтено » | За незнание значительной части программного материала, за существенные ошибки в ответах на вопросы, незнание основных понятий дисциплины. Компетенции, оцениваемые при ответе, не сформированы. |

При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на зачете или экзамене.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены филиалом академии или могут использоваться собственные технические средства.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

| № п/п | Категории студентов | Виды оценочных средств | Форма контроля и оценки результатов обучения |
|--------------|--|-------------------------------------|--|
| 1 | С нарушением слуха | Письменные работы, вопросы к зачету | Преимущественно письменная проверка |
| 2 | С нарушением зрения | Собеседование по вопросам к зачету | Преимущественно устная проверка (индивидуально) |
| 3 | С нарушением опорно – двигательного аппарата | Письменные работы к зачету | Организация взаимодействия обучающихся с помощью электронной почты, письменная проверка. |

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся:

а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме);

б) доступная форма предоставления знаний оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в форме электронного документа);

в) доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, устно).

При необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.

11. ЛИСТ ВНЕСЕНИЯ ИЗМЕНЕНИЙ В РАБОЧУЮ ПРОГРАММУ УЧЕБНОЙ ДИСЦИПЛИНЫ

Дополнения и изменения в программу учебной дисциплины «Информационная безопасность, защита персональных данных» по направлению подготовки _____ на учебный год.

В программу учебной дисциплины вносятся следующие изменения:

- 1.
- 2.
- 3.

Изменения в рабочую программу учебной дисциплины внесены:

Должность,

Звание преподавателя _____ ФИО

Внесение изменений в рабочую программу учебной дисциплины утверждены на заседании кафедры « _____ »

Протокол № ____ от _____. 20__ года.

Зав. кафедрой _____ ФИО