федеральное государственное бюджетное образовательное учреждение высшего образования «Мордовский государственный педагогический университет имени М.Е. Евсевьева»

Физико-математический факультет

Кафедра информатики и вычислительной техники

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность и защита информации

Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки)
Профиль подготовки: Информатика. Экономика
Форма обучения: Очная

Разработчики: Зубрилин А. А., канд. филос. наук, заведующий кафедрой информатики и вычислительной техники, Золотарева Т.П., старший преподаватель

Программа рассмотрена и утверждена на заседании кафедры, протокол № 9 от 17.03.2022 года

Зав. кафедрой _____ Зубрилин А. А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины – формирование навыков организации безопасной работы на персональном компьютере и в компьютерной сети, умений противостоять информационным угрозам, включая технические, технологические, психологические, социальные.

Задачи дисциплины:

- формирование знаний в области российского правового регулирования информационной безопасности, включая защиту персональных данных;
- выработка представлений о способах обеспечения защиты компьютера и противостоянии методам социальной инженерии;
- освоение программных средств обеспечения информационной безопасности при работе на персональном компьютере и в компьютерной сети, включая формирование умений аргументированного выбора и самостоятельной установки соответствующего программного обеспечения;
- обучение основам криптографии как одного из средств шифрования данных

В том числе воспитательные задачи:

- формирование мировоззрения и системы базовых ценностей личности;
- формирование основ профессиональной культуры обучающегося в условиях трансформации области профессиональной деятельности.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина К.М.07.14 «Информационная безопасность и защита информации» изучается на 5 курсе, в 10 семестре.

Для изучения дисциплины требуется: основ защиты информации, владение информационными технологиями.

Изучению дисциплины «Информационная безопасность и защита информации» предшествует освоение дисциплин (практик):

Программное обеспечение систем и сетей;

Архитектура компьютера.

Освоение дисциплины К.М.07.14 «Информационная безопасность и защита информации» является необходимой основой для последующего изучения дисциплин (практик):

Интернет-технологии.

Область профессиональной деятельности, на которую ориентирует дисциплина «Информационная безопасность и защита информации», включает:

01 Образование и наука (в сфере дошкольного, начального общего, основного общего, среднего общего образования, профессионального обучения, профессионального образования, дополнительного образования).

Типы задач и задачи профессиональной деятельности, к которым готовится обучающийся, определены учебным планом.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Компетенция в соответствии ФГОС ВО	
Индикаторы достижения компетенций	**Образовательные результаты**
ПК-1. Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач.	
ПК-1.1. Знает структуру, состав и дидактические единицы	знать: - основные определения и базовые понятия научной

предметной области (преподаваемого предмета)	области «Информационная безопасность»; - основные тенденции развития информационных технологий, связанных с обеспечением информационной безопасности в образовательных организациях; уметь: - аргументировано выбирать и эффективно использовать программные средства для обеспечения информационной безопасности компьютера; - оценивать программное обеспечение для обеспечения информационной безопасности и перспективы его использования с учетом решаемых профессиональных задач; владеть: - средствами обеспечения информационной безопасности при работе за персональным компьютером и в компьютерных сетях.
ПК-1.2. Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО	знать: - способы шифрования данных; - возможные технические, технологические, социальные угрозы, связанные с компьютерной техникой; уметь: - определять оптимальный набор программных средств для обеспечения безопасной работы на компьютере и в компьютерных сетях; владеть: - навыками отбора программных средств для изучения школьниками основ информационной безопасности.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Десятый семестр
Контактная работа (всего)	**42**	**42**
Лекции	14	14
Практические	28	28
Самостоятельная работа (всего)	**30**	**30**
Виды промежуточной аттестации		
Зачет	+	+
Общая трудоемкость часы	**72**	**72**
Общая трудоемкость зачетные единицы	**2**	**2**

5. Содержание дисциплины

5.1. Содержание разделов дисциплины

Раздел 1. Теоретико-правовые вопросы защиты информации в компьютерных сетях:

Общие вопросы информационной безопасности. Определение и эволюция понятия «информационная безопасность». Цели, задачи, направления информационной безопасности. Базовые принципы обеспечения информационной безопасности. Информационная безопасность в условиях функционирования в России глобальных сетей. Нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Персональные данные как вид защищаемой информации. Законодательство о

безопасности и защите информации, его структура и содержание. Авторское право. Интеллектуальная собственность.

Раздел 2. Программные и технические средства защиты информации. Комплексное обеспечение информационной безопасности в образовательных организациях:

Вредоносное программное обеспечение и меры защиты от него. Понятие о видах вирусов. Антивирусная защита компьютера. Технология построения защищенных информационных систем.

Парольная защита. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство защиты от несанкционированного доступа. Средства родительского контроля.

Средства контроля доступа в информационных системах. Технические средства защиты информации. Механические системы защиты информации. Электронные ключи и замки. Биометрические системы идентификации.

Основные этапы обеспечения защиты информации: определение политики и составляющих информационной безопасности, управление рисками, аудит информационной безопасности. Меры и методы по защите информации в образовательных организациях.

Анализ и оценивание угроз информационной безопасности личности в цифровой образовательной среде. Интернет-зависимость. Влияние социальных сетей на адаптацию молодежи.

Понятие шифра. Симметричное и ассиметричное шифрование. Односторонние функции. Метод RSA. Электронная подпись.

5.2. Содержание дисциплины: Лекции (14 ч.)

Раздел 1. Теоретико-правовые вопросы защиты информации в компьютерных сетях (6 часов)

Тема 1. Общие вопросы информационной безопасности (2 ч.)

Теоретические вопросы организации информационной безопасности. Международные стандарты информационного обмена. Понятие информационной угрозы. Информационная безопасность как научная область. Направления обеспечения информационной безопасности в современных условиях.

Тема 2. Информационная безопасность в условиях функционирования в России глобальных сетей (2 ч.)

Виды противников или «нарушителей». Нарушение правил информационной безопасности в образовательных организациях. Информационная угроза. Виды информационных угроз. Уровни нарушения информационной безопасности: аппаратный, программный, человеческий фактор. Причины возникновения информационных угроз и меры защиты от них. Основные этапы обеспечения защиты информации: определение политики и составляющих информационной безопасности, управление рисками, аудит информационной безопасности. Меры и методы по защите информации в образовательных организациях

Тема 3. Нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы (2 ч.)

Закон об информации. Судебные прецеденты и ответственность за нарушение закона. Концепция информационной безопасности РФ. Информационная безопасность личности, общества, государства. Персональные данные. Причины несанкционированного доступа к персональным данным. Способы противодействия незаконного доступа к персональным данным. Законодательство в области персональных данных. Закон о персональных данных.

Раздел 2. Программные и технические средства защиты информации. Комплексное обеспечение информационной безопасности в образовательных организациях (8 часов)

Тема 4. Программные средства защиты информации (2 ч.)

Компьютерные вирусы и антивирусная защита. Парольная защита. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство защиты от несанкционированного доступа. Средства родительского контроля.

Тема 5. Технические средства защиты и комплексное обеспечение информационной безопасности (2 ч.)

Средства контроля доступа в информационных системах. Технические средства защиты информации. Механические системы защиты информации. Электронные ключи и замки. Биометрические системы идентификации. Брандмауэр как аппаратное и программное средство ограничения доступа к информации. Программные средства компьютера по обнаружению вторжения и защите от него.

Тема 6. Психологическое воздействие на пользователя как информационная угроза (2 ч.)

Анализ и оценивание угроз информационной безопасности личности в цифровой образовательной среде. Интернет-зависимость. Влияние социальных сетей на адаптацию молодежи. Способы психологического воздействия. Способы защиты от воздействия. Социальная инженерия.

Тема 7. Элементы криптографии (2 ч.)

Криптография как научная область. Генезис криптографии. Криптография и ее место в обеспечении информационной безопасности предприятия. Методы криптографической защиты информации. Программы средства для шифрования данных. Способы шифрования данных. Программы для шифровки и расшифровки данных. Понятие шифра. Симметричное и ассиметричное шифрование. Односторонние функции. Метод RSA. Электронная подпись.

5.3. Содержание дисциплины: Практические (28 ч.)

Раздел 1. Теоретико-правовые вопросы защиты информации в компьютерных сетях (12 часов)

Тема 1. Правовые вопросы, связанные с информационной безопасностью (2 ч.)

Правовое регулирование в области информационной безопасности. Законы о преступлениях в сфере информационных технологий. Авторское право. Пути доказательства авторства.

Тема 2. Интеллектуальная собственность и меры по ее соблюдению (2 ч.)

Интеллектуальная собственность. Способы защиты интеллектуальной собственности. Лицензионное программное обеспечение. Компьютерное пиратство и законодательная ответственность за него. Компьютерные пираты. Способы совершения компьютерного пиратства. Законодательство РФ в области компьютерного пиратства.

Тема 3. Нормативные документы, касающиеся государственной тайны (2 ч.)

Государственная тайна. Ответственность за разглашение государственной тайны. Состояние законодательства РФ в области сохранения государственной тайны.

Тема 4. Нормативные документы, касающиеся государственной тайны (2 ч.)

Решения ситуационных задач на нарушение государственной тайны.

Тема 5. Основы защиты сетевого компьютера от информационных угроз (2 ч.)

Проблемы выбора защитного программного обеспечения. Сайты с бесплатным программным обеспечением по защите компьютера. Обзор программных средств для защиты объектов операционной системы. Брандмауэр как аппаратное и программное средство ограничения доступа к информации. Технология отражения атак брандмауэром. Настройка встроенного брандмауэра Windows. Характеристики специализированных брандмауэров. Критерии отбора брандмауэров для практического использования.

Тема 6. Фильтрация сетевого контента (2 ч.)

Компьютерные программы фильтрации от информационных угроз Интернета. Способы фильтрация данных. Программы контентной фильтрации.

Раздел 2. Программные и технические средства защиты информации. Комплексное обеспечение информационной безопасности в образовательных организациях (16 часов)

Тема 7. Программные и технические средства, связанные с угрозой обеспечения информационной безопасности (2 ч.)

Несанкционированный доступ к аппаратным средствам компьютера и средства ограничения доступа. Взлом экранной заставки Windows и пароля BIOS. Способы предотвращения взлома. Взлом операционной системы посредством носителей информации. Способы защиты. USB-накопители как информационная угроза. Ограничение доступа к USB-накопителям. Разграничение доступа в локальных сетях. Взлом учетных записей пользователей локальной сети. Способы предотвращения взлома.

Тема 8. Программные средства компьютера по обнаружению несанкционированного вторжения и защите от вторжения (2 ч.)

Проактивные системы защиты компьютера. Системы контроля целостности данных. Борьба с потенциально опасными программами.

Тема 9. Понятие о видах вирусов. Антивирусная защита компьютера (2 ч.)

Компьютерный вирус: определение, природа возникновения. Способы попадания вирусов в компьютерную систему. Классификация вирусов. Способы защиты от вирусов. Функциональные возможности антивирусных программных средств. Компьютерная реклама как инструмент заражения компьютера. Руткиты. Клавиатурные шпионы (кейлоггеры). Онлайн инструменты для антивирусной защиты информации. Онлайн-антивирусы. Обзор онлайн-антивирусов. Способы работы. Sms-блокеры и методы борьбы с ними.

Тема 10. Парольная защита (2 ч.)

Пароль как средство ограничения доступа к ресурсу. Требования к выбору пароля. Хранители паролей. Программы восстановления (взлома) паролей. Брутфорс.

Тема 11. Программы шифрования данных (2 ч.)

Шифрование данных и его назначение. Алгоритмы и стандарты шифрования. Архивирование файлов с паролем как инструмент защиты от несанкционированного доступа. Восстановление данных. Грамотное удаление информации с компьютера.

Тема 12. Социальная инженерия и ее методы (4 ч.)

Обзор методов социальной инженерии. Методы и методики психологического воздействия на личность (универсальный сеанс связи, сообщение о проверке почты, сообщение от имени администратора, квитанция о доставке, обличение и др.). Антропогенные инструменты защиты от методов социальной инженерии (привлечение к вопросам безопасности, изучение и внедрение необходимых методов и действий для повышения защиты информационного обеспечения). Обратная социальная инженерия. Фарминг как инструмент скрытого перенаправления на поддельные сайты. Фишинг и вишинг как инструмент получения конфиденциальной информации. Мошенничество в Интернете. Правила поведения пользователей в сети Интернет при работе с информационными ресурсами.

Тема 13. Социальные сети как информационная угроза (2 ч.)

Социальная сеть как инструмент сбора информации о гражданине. Инициируемые и не инициируемые пользователем угрозы в социальных сетях. Меры защиты от информационных угроз в социальной сети.

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (разделу)

6.1 Вопросы и задания для самостоятельной работы

Десятый семестр (30 ч.)

Раздел 1. Теоретико-правовые вопросы защиты информации в компьютерных сетях (14 ч.)

Вид СРС: * Выполнение индивидуальных заданий

Подготовка ситуационных задач по информационной безопасности на основании статейсоответствующих законов и нормативных актов РФ.

Возможные разделы:

Раздел «АВТОРСКОЕ ПРАВО» ГК РФ ч. IV:

Статья 1255. Авторские права

Статья 1256. Действие исключительного права на произведения науки, литературы и искусства на территории Российской Федерации

Статья 1265. Право авторства и право автора на имя

Статья 1266. Право на неприкосновенность произведения и защита произведения от искажений

Статья 1267. Охрана авторства, имени автора и неприкосновенности произведения после смерти автора

Статья 1270. Исключительное право на произведение

Статья 1274. Свободное использование произведения в информационных, научных, учебных или культурных целях

Статья 1286. Лицензионный договор о предоставлении права использования произведения

Статья 1286.1. Открытая лицензия на использование произведения науки, литературы или искусства

Статья 1290. Ответственность по договорам, заключаемым автором произведения

Статья 1295. Служебное произведение

Статья 1296. Произведения, созданные по заказу

Статья 1297. Произведения, созданные при выполнении работ подоговору

Статья 1299. Технические средства защиты авторских прав

Статья 1301. Ответственность за нарушение исключительного права на произведение

Статья 1302. Обеспечение иска по делам о нарушении авторских прав УК РФ:

Статья 146. Нарушение авторских и смежных прав

Статья 147. Нарушение изобретательских и патентных прав

КоАП РФ:

Статья 7.12. Нарушение авторских и смежных прав, изобретательских и патентных прав ФЗ РФ «Об авторском праве и смежных правах»:

Статья 17. Право доступа к произведениям изобразительного искусства. Право наследования

Статья 26. Воспроизведение произведения в личных целях без согласия автора с выплатой авторского вознаграждения

Статья 39. Использование фонограммы, опубликованной в коммерческих целях, без согласия производителя фонограммы и исполнителя

Статья 48. Нарушение авторских и смежных прав. Контрафактные экземпляры произведения и фонограммы

Статья 49. Гражданско-правовые способы защиты авторского права и смежныхправ

Раздел «ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ»

ГК РФ:

Статья 1246. Государственное регулирование отношений в сфере интеллектуальной собственности

УК РФ

Статья 159.6. Мошенничество в сфере компьютерной информации

Раздел «ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ» УК РФ

Статья 272. Неправомерный доступ к компьютерной информации

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

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачикомпьютерной информации и информационно-телекоммуникационных сетей

Раздел «ПРЕСТУПЛЕНИЯ ПРОТИВ ГОСУДАРСТВЕННОЙ ВЛАСТИ»

Закон РФ «О государственной тайне»

Статья 5. Перечень сведений, составляющих государственную тайну

Статья 16. Взаимная передача сведений, составляющих государственную тайну, органамигосударственной власти, предприятиями, учреждениями и организациями

Статья 19. Защита сведений, составляющих государственную тайну, при изменении функций субъектов правоотношений

Статья 21. Допуск должностных лиц и граждан к государственнойтайне

Статья 21.1. Особый порядок допуска к государственной тайне

Статья 22. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне

Статья 24. Ограничения прав должностного лица или гражданина, допущенных или ранеедопускавшихся к государственной тайне

Статья 26. Ответственность за нарушение законодательства Российской Федерации о государственной тайне

УК РФ:

Статья 283. Разглашение государственной тайны

Статья 275. Государственная измена

Статья 276. Шпионаж

КоАП РФ:

Статья 7.31. Нарушение порядка ведения реестра контрактов, заключенных заказчиками, реестра контрактов, содержащего сведения, составляющие государственную тайну, реестра недобросовестных поставщиков (подрядчиков, исполнителей)

Алгоритм разработки задачи:

1. Выбрать и изучить статью из нормативного акта.
2. Проанализировать материалы сайтов, например, http://itsec.ru, на предмет наказания за нарушения в сфере информационной безопасности.
3. Разработать ситуационную задачу и привести ее решение с указанием нормативныхактов, на которые осуществлялась опора.

Пример задачи:

Гражданин Иванов создал антивирусное программное средство под названием «EFVIv» зарегистрировал на него свои права. 20.09.2017 этот гражданин заключил договор с компанией «Saransk-IT» и передал свои имущественные права на распространение своего программного продукта сроком на один год. После заключения договора компания «Saransk-IT» перепродала для распространения версию программы «EFVIv» другой компании без ведома автора. Имеет ли место в данной ситуации нарушение авторского права гражданинаИванова?

Решение.

Согласно статьи 1270 ГК РФ:

Автору произведения или иному правообладателю принадлежит исключительное право использовать произведение в соответствии со статьей 1229 настоящего Кодекса в любой форме и любым не противоречащим закону способом (исключительное право на произведение), в том числе способами, указанными в пункте 2 настоящей статьи. Правообладатель может распоряжаться исключительным правом на произведение.

2. Использованием произведения независимо от того, совершаются ли соответствующие действия в целях извлечения прибыли или без такой цели, считается, в частности: распространение произведения путем продажи или иного отчуждения его оригинала или экземпляров;

Таким образом, в данном случае имеет место нарушение авторского права гражданина Иванова.

Вид СРС: * Выполнение творческих заданий

На свой выбор выполните одно из следующих творческих заданий:

1.) Составьте каталог интернет-ресурсов, полезных для воспитания, образования и развития детей.

2) Осуществите сравнение функций родительского контроля в составе антивирусных программ.

3) Разработайте комплекс мероприятий по защите персональных данных в образовательной организации.

4) Осуществите разработку политики информационной безопасности в образовательной организации.

Раздел 2. Программные и технические средства защиты информации. Комплексное обеспечение информационной безопасности в образовательных организациях (16 ч.)

Вид СРС: *Выполнение индивидуальных заданий

СХЕМА ОФОРМЛЕНИЯ ОПИСАНИЯ ПРИЛОЖНЕНИЯ ДЛЯ ОРГАНИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА КОМПЬЮТЕРЕ

Общие сведения (20 баллов)

Название приложения:

Производитель:

Сайт производителя:

Необходимость инсталляции (да/нет)

Требования к операционной системе и аппаратным ресурсам ПК: Обновление (ручное/автоматическое)

Тип приложения (бесплатное, условно-бесплатное, лицензионное) Функциональные возможности:

Описание приложения (35 баллов) Скриншот приложения

Описание пунктов меню приложения

Настройка приложения (45 баллов)

Описание настройки приложения на работу

Описание этапов работы с приложением по обеспечению информационной безопасности на компьютере

Список приложений для рассмотрения:

Межсетевые экраны (со встроенным и без встроенного антивируса)

AVG

Internet Security

BitDefender

Total Security Norton и др.

Программы проактивной защиты и защиты от шпионских программ

WinPatrol

Ad-Aware

SUPER

AntiSpyware

AVZ и др.

Антивирусные программы и утилиты

Trojan Remover

McAfee AVERT Stinger

RogueKiller

Trojan Killer

Immunos

Emsisoft Anti-Malware

Remove Fake Antivirus

GMER

AntiSMS

Norman Malware Cleaner

AVG Anti-virus Free Edition

Dr.WEB CureIt!

RegRun Reanimator и др.

Вид СРС: * Выполнение творческих заданий

Напишите эссе объемом 2-3 страницы, в котором изложите свою позицию по одному из следующих вопросов:

1) Биометрические системы идентификации.

2) Безопасность и конфиденциальность в сети Интернет.

3) Понятие о персональных данных.

4) Информация, составляющая коммерческую тайну.

5) Объекты информационной безопасности в предметной области.

6) Информационная среда: иллюзии или реальности

7) Случайные и целенаправленные угрозы нарушения сохранности информации.

8) Понятие дезинформации.

9) Риски информационной безопасности.

10) Информационное оружие.

11) Информационные войны.

12) Технические средства промышленного шпионажа.

13) Противодействие технические средства промышленного шпионажа.

14) Классы безопасности.

15) Аудит информационной безопасности.

16) История хакерства.

17) Хакерство в России.

18) Хакер: мастер или вредитель?

19) Правовые механизмы защиты информации на разных уровнях.

20) Понятие и применение электронной цифровой подписи.

21) Манипуляции сознанием.

22) Манипулятивные механизмы управления личностью.

23) Программы родительского контроля.

24) Вред и польза программ родительского контроля.

25) Средства антивирусной защиты мобильных устройств.

7. Тематика курсовых работ (проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

8. Оценочные средства

8.1 Компетенции и этапы формирования

№ п/п	Оценочные средства	Компетенции, этапы ихформирования
1	Предметно-методический модуль	ПК-1.

8.2 Показатели и критерии оценивания компетенций, шкалы оценивания

Шкала, критерии оценивания и уровень сформированности компетенции			
2 (не зачтено) ниже порогового	3 (зачтено) пороговый	4 (зачтено) базовый	5 (зачтено) повышенный
ПК-1. Способен осваивать и использовать теоретические знания и практические умения и навыки в предметной области при решении профессиональных задач			
ПК-1.1. Знает структуру, состав и дидактические единицы предметной области (преподаваемого предмета)			
Не демонстрирует знание структуры, состава и дидактических единиц предметной области (преподаваемого предмета).	В целом успешно, но бессистемно демонстрирует знание структуры, состава и дидактических единиц предметной области (преподаваемого предмета).	В целом успешно, но с отдельными недочетами демонстрирует знание структуры, состава и дидактических единиц предметной области (преподаваемого предмета).	Демонстрирует в полном объеме знание структуры, состава и дидактических единиц предметной области (преподаваемого предмета).
ПК-1.2. Умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО			
Не умеет осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО.	В целом успешно, но бессистемно демонстрирует умение осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО.	В целом успешно, но с отдельными недочетами демонстрирует умение осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО.	Способен в полном объеме демонстрировать умение осуществлять отбор учебного содержания для его реализации в различных формах обучения в соответствии с требованиями ФГОС ОО.

Уровень сформированности компетенции	Шкала оценивания дляпромежуточной аттестации	Шкала оценивания по БРС
	Зачет	
Повышенный	зачтено	90 – 100%
Базовый	зачтено	76 – 89%
Пороговый	зачтено	60 – 75%
Ниже порогового	не зачтено	Ниже 60%

8.3 Вопросы промежуточной аттестации

Десятый семестр (Зачет, ПК-1.1, ПК-1.2)

1. Раскройте роль информации в современном мире. Дайте понятие о защищаемой информации. Сформулируйте определение защиты информации, укажите основные аспекты защиты информации и обоснуйте их целесообразность.
2. Раскройте понятие «информационная безопасность». Приведите примеры нарушения информационной безопасности на предприятии. Раскройте теорию информационной безопасности. Опишите ее основные направления.
3. Расскажите об обеспечении информационной безопасности и выделите направления защиты.
4. Дайте понятие политики информационной безопасности. Опишите способы организации политики информационной безопасности на предприятии. Приведите требования к системе и политике информационной безопасности.
5. Раскройте законодательный уровень обеспечения информационной безопасности. Выделите основные законодательные акты РФ в области защиты информации. Охарактеризуйте структуру законодательства РФ в области защиты информации.
6. Раскройте Доктрину информационной безопасности РФ в современных условиях.
7. Дайте определение государственной тайны. Перечислите основные статьи в Федеральном Законе о государственной тайне. Расскажите о защите государственной тайны в РФ.
8. Дайте определение понятиям «авторское право» и «коммерческая тайна». Укажите их отличительные особенности. Охарактеризуйте способы защиты авторских прав и коммерческой тайны. Расскажите о защите коммерческой тайны в РФ.
9. Расскажите о защите персональных данных в РФ. Выделите основные направления Закона о персональных данных.
10. Расскажите о защите служебной и профессиональной тайны в РФ.
11. Раскройте процедуру сертификации и аттестации в РФ.
12. Раскройте понятие «информационная угроза» с позиции проблемы обеспечения информационной безопасности на предприятии. Охарактеризуйте виды угроз, приведите примеры. Приведите классификации угроз.
13. Раскройте возможные угрозы нарушения конфиденциальности информации. Выделите особенности и приведите примеры реализации угроз.
14. Раскройте угрозы нарушения целостности информации. Выделите особенности и приведите примеры реализации угроз.
15. Раскройте угрозы нарушения доступности информации. Выделите особенности и приведите примеры реализации угроз.
16. Раскройте источники угроз. Приведите классификации источников угроз.
17. Раскройте понятие идентификации и аутентификации в компьютерных сетях. Расскажите о назначении парольной защиты. Выделите ее недостатки. Опишите на примере конкретного приложения технологию функционирования программных средств, использующихся для создания и хранения паролей.
18. Дайте понятие электронной подписи. Укажите пути ее применения. Раскройте суть электронной цифровой подписи. Охарактеризуйте правовой и технический аспекты.

Сформулируйте рекомендации для использования электронной цифровой подписи.

19. Раскройте организационные меры обеспечения информационной безопасности. Выделите функционал службы безопасности предприятия.

20. Расскажите о программно-аппаратных средствах защиты информации. Охарактеризуйте аппаратные средства защиты информации. Дайте их классификации. Приведите примеры аппаратных средств защиты информации в компьютерной сети предприятия. Опишите межсетевые экраны и антивирусные средства, выделите их функции и назначение.

21. Дайте понятие криптографии как научной области, связанной с шифрованием данных. Приведите примеры шифров. Опишите криптографические меры обеспечения информационной безопасности. Дайте классификацию криптографических алгоритмов.

22. Расскажите о симметричном и ассиметричном шифровании. Выделите принципы симметричного шифрования. Опишите простейшие методы ассиметричного шифрования.

23. Раскройте назначение односторонних функций и их применение при шифровании данных. Расскажите о методе RSA.

24. Опишите социальные сети как инструмент сбора информации о пользователе.

25. Раскройте суть социальной инженерии. Опишите ее методы. Приведите примеры мошенничества в сети Интернет. Раскройте способы противодействия Интернет-мошенникам.

8.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Промежуточная аттестация проводится в форме зачета.

Зачет позволяет оценить сформированность компетенций, теоретическую подготовку студента, его способность к творческому мышлению, готовность к практической деятельности, приобретенные навыки самостоятельной работы, умение синтезировать полученные знания и применять их при решении практических задач.

Итоговая оценка выставляется с учетом набранной суммы баллов.

При оценке достижений студентов необходимо обращать особое внимание на:

– усвоение программного материала;

– умение излагать программный материал научным языком;

– умение связывать теорию с практикой;

– владение навыками поиска, систематизации необходимых источников литературы по дисциплине «Информационная безопасность и защита информации»;

– умение обосновывать принятые решения;

– владение навыками и приемами выполнения практических заданий;

– умение подкреплять ответ иллюстративным материалом.

9. Перечень основной и дополнительной учебной литературы

Основная литература

1. Артемов, А. В. Информационная безопасность [Электронный ресурс] : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. – Орел : МАБИВ, 2014. – 257 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=428605. – Текст : электронный.

2. Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях [Электронный ресурс] : учебное пособие / А. М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=480637. – Текст : электронный.

3. Мэйволд, Э. Безопасность сетей [Электронный ресурс] / Э. Мэйволд. – 2-е изд., испр. М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с. – Режим доступа : //biblioclub.ru/index.php?page=book&id=429035. – Текст : электронный.

Дополнительная литература

1. Авдошин, С.М. Технологии и продукты Microsoft в обеспечении информационной безопасности: курс / С.М. Авдошин, А.А. Савельева, В.А. Сердюк ; Национальный Открытый Университет «ИНТУИТ». – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2010. – 384 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=233684). – Текст : электронный.

2. Сагдеев, К. М. Физические основы защиты информации [Электронный ресурс] : учебноепособие / К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». – Ставрополь : СКФУ, 2015. – 394 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=458285. – Текст : электронный.

3. Технологии защиты информации в компьютерных сетях [Электронный ресурс] / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 369 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=428820. – Текст : электронный.

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://all-ib.ru – Информационная безопасность. Защита информации
2. http://www.securrity.ru – SecuRRity.Ru – «Информационная безопасность компьютерных систем и защита конфиденциальных данных»
3. http://www.securitylab.ru – Security Lab by Positive Technologies

11. Методические указания обучающимся по освоению дисциплины (модуля)

При освоении материала дисциплины необходимо:

– спланировать и распределить время, необходимое для изучения дисциплины;
– конкретизировать для себя план изучения материала;
– ознакомиться с объемом и характером внеаудиторной самостоятельной работы для полноценного освоения каждой из тем дисциплины.

Сценарий изучения курса:

– проработайте каждую тему по предлагаемому ниже алгоритму действий;
– регулярно выполняйте задания для самостоятельной работы, своевременно отчитывайтесь преподавателю об их выполнении;
– изучив весь материал, проверьте свой уровень усвоения содержания дисциплины и готовность к сдаче зачета/экзамена, выполнив задания и ответив самостоятельно на примерные вопросы для промежуточной аттестации.

Алгоритм работы над каждой темой:

– изучите содержание темы вначале по лекционному материалу, а затем по другим источникам;
– прочитайте дополнительную литературу из списка, предложенного преподавателем;
– выпишите в тетрадь основные понятия и категории по теме, используя лекционный материал или словари, что поможет быстро повторить материал при подготовке к промежуточной аттестации;
– составьте краткий план ответа по каждому вопросу, выносимому на обсуждение на аудиторном занятии;
– повторите определения терминов, относящихся к теме;

– продумайте примеры и иллюстрации к обсуждению вопросов по изучаемой теме;

– подберите цитаты ученых, общественных деятелей, публицистов, уместные с точки зрения обсуждаемой проблемы;

– продумывайте высказывания по темам, предложенным к аудиторным занятиям.

Рекомендации по работе с литературой:

– ознакомьтесь с аннотациями к рекомендованной литературе и определите основной метод изложения материала того или иного источника;

– составьте собственные аннотации к другим источникам, что поможет при подготовке рефератов, текстов речей, при подготовке к промежуточной аттестации;

– выберите те источники, которые наиболее подходят для изучения конкретной темы;

– проработайте содержание источника, сформулируйте собственную точку зрения на проблему с опорой на полученную информацию.

12. Перечень информационных технологий

Реализация учебной программы обеспечивается доступом каждого студента к информационным ресурсам – электронной библиотеке и сетевым ресурсам Интернет. Для использования ИКТ в учебном процессе используется программное обеспечение, позволяющее осуществлять поиск, хранение, систематизацию, анализ и презентацию информации, экспорт информации на цифровые носители, организацию взаимодействия в реальной и виртуальной образовательной среде.

Индивидуальные результаты освоения дисциплины студентами фиксируются в электронной информационно-образовательной среде университета.

12.1 Перечень программного обеспечения (обновление производится по мере появления новых версий программы)

1. Microsoft Windows 7 Pro
2. Microsoft Office Professional Plus 2010
3. 1С: Университет ПРОФ

12.2 Перечень информационных справочных систем (обновление выполняется еженедельно)

1. Справочная правовая система «КонсультантПлюс» (http://www.consultant.ru)
2. Информационно-правовая система «ГАРАНТ» (http://www.garant.ru)

12.3 Перечень современных профессиональных баз данных

1. Профессиональная база данных «Открытые данные Министерства образования и науки РФ» (http://xn----8sblcdzzacvuc0jbg.xn--80abucjiibhv9a.xn--p1ai/opendata)
2. Электронная библиотечная система Znanium.com (http://znanium.com)
3. Единое окно доступа к образовательным ресурсам (http://window.edu.ru)

13. Материально-техническое обеспечение дисциплины (модуля)

Для проведения аудиторных занятий необходим стандартный набор специализированной учебной мебели и учебного оборудования, а также мультимедийное оборудование для демонстрации презентаций на лекциях. Для проведения практических занятий, а также организации самостоятельной работы студентов необходим компьютерный класс с рабочими местами, обеспечивающими выход в Интернет.

Индивидуальные результаты освоения дисциплины фиксируются в электронной информационно-образовательной среде университета.

Реализация учебной программы обеспечивается доступом каждого студента к информационным ресурсам – электронной библиотеке и сетевым ресурсам Интернет. Для использования ИКТ в учебном процессе необходимо наличие программного обеспечения,

позволяющего осуществлять поиск информации в сети Интернет, систематизацию, анализ и презентацию информации, экспорт информации на цифровые носители.

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования (выполнения курсовых работ).

Лаборатория вычислительной техники.

Помещение оснащено оборудованием и техническими средствами обучения.

Основное оборудование:

Автоматизированное рабочее место в составе (системный блок, монитор, клавиатура, мышь), интерактивный дисплей.

Лабораторное оборудование: автоматизированное рабочее место (компьютеры – 13 шт.).

Учебно-наглядные пособия:

Презентации.

Помещение для самостоятельной работы.

Помещение оснащено оборудованием и техническими средствами обучения.

Основное оборудование:

Компьютерная техника с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета (персональный компьютер 10 шт.).

Учебно-наглядные пособия:

Презентации.

Помещение для самостоятельной работы.

Читальный зал.

Основное оборудование:

Компьютерная техника с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета (компьютер 10 шт., проектор с экраном 1 шт., многофункциональное устройство 1 шт., принтер 1 шт.)

Учебно-наглядные пособия:

Учебники и учебно-методические пособия, периодические издания, справочная литература.

Стенды с тематическими выставками.