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

Физико-математический факультет

Кафедра информатики и вычислительной техники

РАБОЧАЯПРОГРАММАДИСЦИПЛИНЫ
Основы информационной безопасности

Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки)
Профиль подготовки: Менеджмент в образовании. Информационная безопасность в образовании
Форма обучения: Очная

Разработчик: Зубрилин А.А., канд. филос. наук, доцент, заведующий кафедрой информатики и вычислительной техники

Программа рассмотрена и утверждена на заседании кафедры информатики и вычислительной техники, протокол № 3 от 29.10.2021 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;
- 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.06.24 «Основы информационной безопасности» относится к части учебного плана, формируемой участниками образовательных отношений.

Дисциплина изучается на 1 курсе, в 1 и 2 семестрах.

Для изучения дисциплины требуется: знание возможностей сервисов сети Интернет.

Изучению дисциплины «Основы информационной безопасности» не предшествует освоение никаких дисциплин.

Область профессиональной деятельности, на которую ориентирует дисциплина «Основы информационной безопасности», включает:

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

В процессе изучения дисциплины студент готовится к видам профессиональной деятельности и решению профессиональных задач, предусмотренных ФГОС ВО и 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-11. Способен использовать теоретические и практические знания для постановки и решения исследовательских задач в предметной области (в соответствии с профилем и уровнем обучения) и в области образования.	

педагогическая деятельность

ПК-11.1 Использует теоретические и практические знания для постановки и решения исследовательских	знать: - способы шифрования данных; уметь: - определять оптимальный набор программных средств

задач в предметной области в соответствии с профилем и уровнем обучения и в области образования.	для обеспечения безопасной работы на компьютере; владеть: - средствами обеспечения информационной безопасности при работе за персональным компьютером и в компьютерных сетях.
ПК-14. Способен устанавливать содержательные, методологические и мировоззренческие связи предметной области (в соответствии с профилем и уровнем обучения) со смежными научными областями.	

педагогическая деятельность

ПК-14.1 Обосновывает роль моделирования в сфере менеджмента и информационной безопасности в образовании; владеет современными представлениями о понятийном аппарате, применяемом в предметной области.	знать: - возможные технические, технологические, социальные угрозы, связанные с компьютерной техникой; - способы шифрования данных; - применение шифрования данных в различных областях естествознания; уметь: - аргументировано выбирать и эффективно использовать программные средства для обеспечения информационной безопасности компьютера; владеть: - средствами обеспечения информационной безопасности приработе за персональным компьютером и в компьютерных сетях.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Первый семестр	Второй семестр
Контактная работа (всего)	**72**	**36**	**36**
Лекции	36	18	18
Практические	36	18	18
Самостоятельная работа (всего)	**64**	**72**	**18**
Виды промежуточной аттестации	**18**		**18**
Зачет		+	
Экзамен			18
Общая трудоемкость часы	**180**	**108**	**72**
Общая трудоемкость зачетные единицы	**5**	**3**	**2**

5. Содержание дисциплины

5.1. Содержание разделов дисциплины

Раздел 1. Правовые вопросы защиты информации в компьютерных сетях:

Общие вопросы информационной безопасности. Информационные ресурсы по информационной безопасности. Информационная безопасность в условиях функционирования в России глобальных сетей. Нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

Раздел 2. Программные средства и сервисы сети Интернет по защите информации

Информационная безопасность как наука и деятельность. Виды возможных нарушений информационной безопасности. Хакерство как угроза информационной безопасности. DoS- и DDoS-атаки как инструмент ограничения доступа к сетевому

компьютеру. Комплексная защита сетевого компьютера от информационных угроз.

Раздел 3. Практические вопросы организации информационной безопасности в компьютерных сетях:

Вредоносное программное обеспечение и меры защиты от него. Понятие о видах вирусов. Антивирусная защита компьютера. Технология построения защищенных информационных систем. Политика информационной безопасности и ее организация в локальной сети.

Раздел 4. Проблемы информационной безопасности в современном обществе:

Психологическое воздействие на пользователя как информационная угроза. Безопасность персональных данных. Криптография и ее методы шифрования информации. Электронная подпись и правовое обеспечение безопасности переписки. Назначение и задачи обеспечения информационной безопасности на уровне государства.

5.2. Содержание дисциплины:

1 семестр. Лекции (18 ч.)

Раздел 1 Проблемы информационной безопасности в современном обществе (8 ч.)

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

Теоретические вопросы организации информационной безопасности. Пути организации информационной безопасности на предприятии. Информационные ресурсы по информационной безопасности. Международные стандарты информационного обмена. Понятие информационной угрозы.

Тема 2. Информационные ресурсы по информационной безопасности (2 ч.)

Информационная безопасность как научная область. Направления обеспечения информационной безопасности в современных условиях.

Тема 3. Информационная безопасность в условиях функционирования в России глобальных сетей (2 ч.)

Виды противников или «нарушителей». Нарушение правил информационной безопасности в образовательных организациях.

Тема 4. 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.

Раздел 2. Программные средства и сервисы сети Интернет по защите информации (10 ч.)

Тема 5. Информационная безопасность как наука и деятельность (2 ч.)

Понятие и принципы информационной безопасности. Общие термины и определения.

Тема 6. Виды возможных нарушений информационной безопасности (2 ч.)

Информационная угроза. Виды информационных угроз. Уровни нарушения информационной безопасности: аппаратный, программный, человеческий фактор. Причины возникновения информационных угроз и меры защиты от них.

Тема 7. Хакерство как угроза информационной безопасности (2 ч.)

Хакинг и антихакинг. Хакерские технологии. Противостояние хакерству.

Тема 8. DoS- и DDoS-атаки как инструмент ограничения доступа к сетевому компьютеру (2 ч.)

Назначение DoS- и DDoS-атак. Способы организации DoS- и DDoS-атак. Инструменты защиты сайтов от DoS- и DDoS-атак.

Тема 9. Комплексная защита сетевого компьютера от информационных угроз (2 ч.)

Брандмауэр как аппаратное и программное средство ограничения доступа к информации. Программные средства компьютера по обнаружению вторжения и защите от него.

2 семестр. Лекции (18 ч.)

Раздел 3. Практические вопросы организации информационной безопасности в компьютерных сетях (8 ч.)

Тема 10. Вредоносное программное обеспечение и меры защиты от него (2 ч.)

Вирусы. Черви. Программы-шпионы. Рекламное программное обеспечение. Троянские кони.

Тема 11. Понятие о видах вирусов. Антивирусная защита компьютера (2 ч.)

Компьютерные вирус: определение, природа возникновения. Способы попадания вирусов в компьютерную систему. Классификация вирусов. Способы защиты от вирусов.

Тема 12. Технология построения защищенных информационных систем (2 ч.)

Технология определения путей организации защиты информационной системы. Отбор программных средств для организации защиты. Аутентификации пользователей. Распределение прав в информационной системе.

Тема 13. Политика информационной безопасности и ее организация в локальной сети (2 ч.)

Настройка безопасности групповой работы с информационными ресурсами в локальной сети. Локальная политика безопасности. Авторизация и ее задачи. Настройка аудита сетевых ресурсов. Работа с журналом безопасности. Защита локальной сети от взлома. Сниффинг.

Раздел 4. Проблемы информационной безопасности в современном обществе (10 ч.)

Тема 14. Психологическое воздействие на пользователя как информационная угроза (2 ч.)

Способы психологического воздействия. Способы защиты от воздействия.

Тема 15. Безопасность персональных данных (2 ч.)

Персональные данные. Причины несанкционированного доступа к персональным данным. Способы противодействия незаконного доступа к персональным данным. Законодательство в области персональных данных.

Тема 16. Криптография и ее методы шифрования информации (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.

Тема 17. Электронная подпись и правовое обеспечение безопасности переписки (2 ч.)

Виды электронных подписей и принципы их использования. Условия признания электронных документов. Удостоверяющий центр. Полномочия федеральных органов исполнительной власти в сфере использования электронной подписи.

Тема 18. Назначение и задачи обеспечения информационной безопасности на уровне государства (2 ч.)

Государственная защита информации. Законы, регулирующие обеспечение информационной безопасности на уровне государства. Ответственность за нарушение законов.

1 семестр. Практические занятия (18 ч.)

Раздел 1 Проблемы информационной безопасности в современном обществе (8 ч.)

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.

Раздел 2. Программные средства и сервисы сети Интернет по защите информации (10 ч.)

Тема 5. Программные и аппаратные 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.

Тема 6. Программные и аппаратные средства, связанные с угрозой обеспечения информационной безопасности (2 ч.)

USB-накопители на информационная угроза. Ограничение доступа к USB-накопителям. Разграничение доступа в локальных сетях. Взлом учетных записей пользователейлокальной сети. Способы предотвращения взлома.

Тема 7. DoS- и DDoS-атаки как инструмент ограничения доступа к сетевому ресурсу (2 ч.)

Технология проведения DoS- и DDoS-атак (перенаправление трафика, навязывание длинной сетевой маски). Способы предотвращения DoS- и DDoS-атак. Пассивная и активная оборона при защите сервера от атак. Программные средства и информационные ресурсы для отражения DoS- и DDoS- атак.

Тема 8. Комплексная защита 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 9. Программные средства компьютера по обнаружению несанкционированноговторжения и защите от вторжения (2 ч.)

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

2 семестр. Практические (18 ч.)

Раздел 3. Практические вопросы организации информационной безопасности в компьютерных сетях (8 ч.)

Тема 10. 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

Тема 11. Антивирусные программные средства офисного и домашнего назначения (2 ч.)

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 12. Парольная защита (2 ч.)

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

Тема 13. 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.

Раздел 4. Проблемы информационной безопасности в современном обществе (10 ч.)

Тема 14. Социальная инженерия и ее методы (2 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.

Тема 15. Социальная инженерия и ее методы (2 ч.)

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 16. Электронная валюта (2 ч.)

Электронная наличность. Обзор платежных онлайн-систем. Опасности при работе с электронной наличностью. Проблемы электронной оплаты. Способы заработка в Интернете.

Тема 17. 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.

Тема 18. Фильтрация сетевого контента (2 ч.)

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

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

6.1 Вопросы и задания для самостоятельной работы

Первый семестр (72 ч.)

Раздел 1. Проблемы информационной безопасности в современном обществе (36 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.

Раздел 2. Программные средства и сервисы сети Интернет по защите информации (36 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

Spyware Doctor

AVZ и др.

Второй семестр (18 ч.)

Раздел 3. Практические вопросы организации информационной безопасности в компьютерных сетях (12 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

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.

Раздел 4. Проблемы информационной безопасности в современном обществе (6 ч.)

Вид СРС: *Подготовка к промежуточной аттестации

Повторить вопросы, связанные с организацией безопасной работы в компьютерной сети.

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 их формирования
1.	Предметно-методический модуль	ПК-11, ПК-14
2.	Учебно-исследовательский модуль	ПК-11, ПК-14

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-11 Способен использовать теоретические и практические знания для постановки и решения исследовательских задач в предметной области (в соответствии с профилем и уровнем обучения) и в области образования			
ПК-11.1 Использует теоретические и практические знания для постановки и решения исследовательских задач в предметной области в соответствии с профилем и уровнем обучения и в области образования.			
Не способен использовать теоретические и практические знаниядля постановки и решения исследовательских задач в предметной области в соответствии с профилем и уровнемобучения и в области образования.	В целом успешно, нобессистемно использует теоретические и практические знаниядля постановки и решения исследовательских задач в предметной области в соответствии с профилем и уровнемобучения и в области образования.	В целом успешно, нос отдельными недочетами использует теоретические и практические знаниядля постановки и решения исследовательских задач в предметной области в соответствии с профилем и уровнемобучения и в области образования.	Способен в полном объеме использовать теоретические и практические знаниядля постановки и решения исследовательских задач в предметной области в соответствии с профилем и уровнемобучения и в области образования.
ПК-14 Способен устанавливать содержательные, методологические и мировоззренческие связи предметной области (в соответствии с профилем и уровнем обучения) со смежными научными областями			
ПК-14.1 Обосновывает роль моделирования в сфере менеджмента и информационной безопасности в образовании; владеет современными представлениями о понятийном аппарате, применяемом в предметной области.			

Не способен проводить моделирование ситуаций в сфере менеджмента и информационной безопасности в образовании; не владеет современными представлениями о понятийном аппарате, применяемом в предметной области.	В целом успешно, но бессистемно проводит моделирование ситуаций в сфере менеджмента и информационной безопасности в образовании; слабо владеет современными представлениями о понятийном аппарате, применяемом в предметной области.	В целом успешно, но с отдельными недочетами проводит моделирование ситуаций в сфере менеджмента и информационной безопасности в образовании; владеет современными представлениями о понятийном аппарате, применяемом в предметной области.	Способен в полном объеме проводить моделирование ситуаций в сфере менеджмента и информационной безопасности в образовании; не владеет современными представлениями о понятийном аппарате, применяемом в предметной области.

Уровень сформированности компетенции	Шкала оценивания для промежуточной аттестации		Шкала оценивания по БРС
	Экзамен (дифференцированный зачет)	Зачет	
Повышенный	5 (отлично)	зачтено	90 – 100%
Базовый	4 (хорошо)	зачтено	76 – 89%
Пороговый	3 (удовлетворительно)	зачтено	60 – 75%
Ниже порогового	2 (неудовлетворительно)	незачтено	Ниже 60%

8.3 Вопросы промежуточной аттестации

Первый семестр (Зачет, ПК-11.1, ПК -14.1)

1. Сформулируйте определение защиты информации, укажите основные аспекты защиты информации и обоснуйте их целесообразность.
2. Охарактеризуйте структуру законодательства РФ в области защиты информации.
3. Перечислите нормативно-правовые документы, ориентированные на обеспечение информационной безопасности в России. Охарактеризуйте материалы, представленные в этих документах.
4. Дайте определение государственной тайны. Перечислите основные статьи в Федеральном Законе о государственной тайне.
5. Дайте определение понятиям «авторское право» и «коммерческая тайна». Укажите их отличительные особенности. Охарактеризуйте способы защиты авторских прав и коммерческой тайны.
6. Перечислите виды конфиденциальной информации. Приведите примеры конфиденциальной информации и укажите способы ее защиты.
7. Перечислите нормативно-правовые акты, регламентирующие обращение с персональными данными. Приведите примеры внутренних нормативных актов на предприятии о персональных данных.
8. Раскройте понятие «информационная безопасность». Приведите примеры нарушения информационной безопасности на предприятии.
9. Дайте понятие политики информационной безопасности. Опишите способы организации политики информационной безопасности на предприятии.
10. Расскажите о программных средствах, используемых для организации информационной безопасности при работе на компьютере.

11. Расскажите о программных средствах, используемых для организации информационной безопасности при работе в компьютерной сети.

12. Охарактеризуйте аппаратные средства защиты информации. Дайте их классификации. Приведите примеры аппаратных средств защиты информации в компьютерной сети предприятия.

13. Раскройте основные направления организации информационной безопасности. Сформулируйте рекомендации для организации информационной безопасности при работе на компьютере для сотрудников предприятия.

14. Раскройте основные направления организации информационной безопасности в компьютерной сети предприятия. Сформулируйте рекомендации для организации информационной безопасности при работе на сетевом компьютере для сотрудников предприятия.

15. Приведите способы несанкционированного проникновения на сетевой компьютер предприятия и расскажите о путях противодействия проникновению.

16. Раскройте понятие «информационная угроза» с позиции проблемы обеспечения информационной безопасности на предприятии. Охарактеризуйте виды угроз, приведите примеры.

17. Раскройте суть нормативно-правового аспекта защиты информации на предприятии.

18. Раскройте административные вопросы, регламентирующие деятельность предприятия по организации информационной безопасности.

19. Раскройте правовые вопросы, регламентирующие деятельность предприятия по организации информационной безопасности.

20. Охарактеризуйте организационные меры защиты информации на предприятии. Обоснуйте основные мероприятия по обеспечению информационной безопасности.

21. Охарактеризуйте технологические меры информационной безопасности на предприятии. Обоснуйте классификацию средств технологической защиты информации.

22. Опишите технологию функционирования брандмауэров. Раскройте технологию настройки брандмауэра на примере конкретного приложения.

23. Расскажите о проактивных системах защиты компьютера. Приведите примеры программ данного класса.

24. Раскройте понятие «сетевой атаки». Приведите примеры сетевых атак на корпоративную сеть. Укажите пути противодействия сетевым атакам.

25. Расскажите о системах отражения сетевых атак. Опишите их виды, принципы функционирования.

26. Опишите принципы организации DoS- и DoSS-атак. Расскажите о способах борьбы с данным видом информационной угрозы.

27. Опишите принципы организации DoS- и DoSS-атак. Расскажите об облачных технологиях как способе борьбы с данным видом информационной угрозы.

28. Расскажите о системах отражения сетевых атак. Опишите их виды, принципы функционирования.

Второй семестр (экзамен, ПК-11.1, ПК -14.1)

1. Раскройте понятие «информационная угроза» с позиции проблемы обеспечения информационной безопасности на предприятии. Охарактеризуйте виды угроз, приведите примеры.

2. Раскройте суть нормативно-правового аспекта защиты информации на предприятии.

3. Раскройте административные вопросы, регламентирующие деятельность предприятия по организации информационной безопасности.

4. Раскройте правовые вопросы, регламентирующие деятельность предприятия по организации информационной безопасности.

5. Раскройте основные направления организации информационной безопасности. Сформулируйте рекомендации для организации информационной безопасности при работе на компьютере для сотрудников предприятия.

6. Раскройте основные направления организации информационной безопасности в компьютерной сети предприятия. Сформулируйте рекомендации для организации информационной безопасности при работе на сетевом компьютере для сотрудников предприятия.

7. Дайте понятие политики информационной безопасности. Опишите способы организации политики информационной безопасности на предприятии

8. Приведите способы несанкционированного проникновения на сетевой компьютер предприятия и расскажите о путях противодействия проникновению.

9. Охарактеризуйте организационные меры защиты информации на предприятии. Обоснуйте основные мероприятия по обеспечению информационной безопасности.

10. Охарактеризуйте технологические меры информационной безопасности на предприятии. Обоснуйте классификацию средств технологической защиты информации.

11. Расскажите о программных средствах, используемых для организации информационной безопасности при работе на компьютере.

12. Расскажите о программных средствах, используемых для организации информационной безопасности при работе в компьютерной сети.

13. Охарактеризуйте аппаратные средства защиты информации. Дайте их классификации. Приведите примеры аппаратных средств защиты информации в компьютерной сети предприятия.

14. Раскройте понятие «компьютерный вирус». Опишите виды компьютерных вирусов, укажите способы их проникновения на компьютер.

15. Опишите технологию функционирования антивирусных программных средств. Раскройте технологию настройки антивируса на примере конкретного приложения.

16. Раскройте технологию антивирусной защиты сетевого компьютера.

17. Дайте понятие криптографии как научной области, связанной с шифрованием данных. Приведите примеры шифров.

18. Опишите программные средства шифрования данных. Объясните технологию шифрования на примере конкретного приложения.

19. Опишите способы шифрования данных. Раскройте технологию шифрования на примере одного из способов.

20. Опишите на примере конкретного приложения технологию функционирования программных средств, использующихся для создания и хранения паролей.

21. Раскройте сущность потенциально опасных программ. Опишите способы борьбы с ними.

22. Расскажите о системах контроля целостности. Приведите примеры программ данного класса

23. Расскажите о спаме как не затребованной Интернет-рекламе. Приведите способы борьбы со спамом.

24. Расскажите о программах ограничения доступа в Интернет и фильтрации информационных ресурсов.

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

26. Дайте понятие хакинга. Приведите характеристику хакеру как лицу, пытающемуся незаконно завладеть конфиденциальной информацией.

27. Раскройте суть социальной инженерии. Опишите ее методы.

28. Раскройте сущность электронной наличности. Приведите примеры возможной потери электронных денег при совершении платежей в сети Интернет.

29. Приведите примеры мошенничества в сети Интернет. Раскройте способы противодействия Интернет-мошенникам.

30. Раскройте цели и задач криптографии как научной области. Перечислите основные направления использования криптографических методов для защиты информации.

31. Охарактеризуйте современные криптосистемы. Продемонстрируйте модели симметричных и асимметричных криптосистем. Приведите примеры.

32. Охарактеризуйте программные средства шифрования данных. Раскройте технологию шифрования на примере конкретного приложения.

33. Раскройте суть идентификация и аутентификация при входе в информационную систему предприятия. Сформулируйте рекомендации по использованию парольных схем в компьютерных сетях предприятия. Укажите недостатки парольных схем.

34. Раскройте суть электронной цифровой подписи. Охарактеризуйте правовой и технический аспекты. Сформулируйте рекомендации для использования электронной цифровой подписи.

35. Охарактеризуйте программные средства ограничения доступа в Интернет, фильтрации информационных ресурсов. На примере одного приложения раскройте его функциональные возможности по ограничению доступа в Интернет.

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

Промежуточная аттестация проводится в форме зачета и экзамена.

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.

Экзамен 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.

Устный ответ на зачете

Для оценки сформированности компетенции посредством устного ответа студенту предварительно предлагается перечень вопросов или комплексных заданий, предполагающих умение ориентироваться в проблеме, знание теоретического материала, умения применять его в практической профессиональной деятельности, владение навыками и приемами выполнения практических заданий.

Устный ответ на экзамене

Для оценки сформированности компетенции посредством собеседования (устного опроса) студенту предварительно предлагается перечень вопросов или комплексных заданий, предполагающих умение ориентироваться в проблеме, знание теоретического материала, умения применять его в практической профессиональной деятельности, владение навыками и приемами выполнения практических заданий.

При оценке достижений студентов необходимо обращать особое внимание на:

– усвоение программного материала;

– умение излагать программный материал научным языком;

– умение связывать теорию с практикой;

– умение отвечать на видоизмененное задание;

– владение навыками поиска, систематизации необходимых источников литературы по изучаемой проблеме;

– умение обосновывать принятые решения;

– владение навыками и приемами выполнения практических заданий;

– умение подкреплять ответ иллюстративным материалом. Тесты

При определении уровня достижений студентов с помощью тестового контроля необходимо обращать особое внимание на следующее:

– оценивается полностью правильный ответ;

– преподавателем должна быть определена максимальная оценка за тест, включающий определенное количество вопросов;

– преподавателем может быть определена максимальная оценка за один вопрос теста;

– по вопросам, предусматривающим множественный выбор правильных ответов, оценка определяется исходя из максимальной оценки за один вопрос теста.

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;

– изучив весь материал, выполните итоговый тест, который продемонстрирует готовность к сдаче зачета.

Алгоритм работы над каждой темой:

– изучите содержание темы вначале по теоретическому материалу, а затем подругим источникам;

– прочитайте дополнительную литературу из списка, предложенного преподавателем;

– составьте краткий план ответа по каждому вопросу, выносимому на обсуждение на занятии;

– выучите определения терминов, относящихся к теме;

– продумайте примеры и иллюстрации к ответу по изучаемой теме;

– продумывайте высказывания по темам, предложенным к лабораторному занятию.

Рекомендации по работе с литературой:

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

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

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

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)

2.1 Перечень современных профессиональных баз данных

1. Профессиональная база данных «Открытые данные Министерства образования и наукиРФ» (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, экспортинформации на цифровые носители.

Учебная аудитория для проведения учебных занятий.

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Лаборатория вычислительной техники.

Помещение оснащено оборудованием и техническими средствами обучения.Основное оборудование:

Автоматизированное рабочее место в составе (системный блок, монитор, клавиатура, мышь, гарнитура, проектор, интерактивная доска), магнитно-маркерная доска.

Лабораторное оборудование: автоматизированное рабочее место (компьютеры – 24 шт.).

Учебно-наглядные пособия:

Презентации.