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

Факультет иностранных языков
Кафедра информатики и вычислительной техники

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Наименование дисциплины (модуля): Основы информационной безопасности в профессиональной деятельности
Уровень ОПОП: Специалитет

Специальность: 45.05.01 Перевод и переводоведение
Специализация: Лингвистическое обеспечение межгосударственных отношений
Форма обучения: Очная

Разработчик:
Лапин К. С., канд. физ.-мат. наук, доцент

Программа рассмотрена и утверждена на заседании кафедры, протокол № 13 от 17.05.2018 года

Зав. кафедрой _____ _____Вознесенская Н. В.

Программа с обновлениями рассмотрена и утверждена на заседании кафедры, протокол № 1 от 31.08.2020 года

Зав. кафедрой _____ _____Зубрилин А. А.

Подготовлено в системе 1С:Университет (000015030)

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины – формирование способность организовывать безопасную работу на персональном компьютере и в компьютерной сети, 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;
- обзор криптографических методов шифрования данных;
- выработка умений разрабатывать и реализовывать политику информационной безопасности на предприятии;
- формирование способностей по противодействию мошенническим действиям в сети Интернет и ведения просветительской работы в этом направлении.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина Б1.Б.09 «Основы информационной безопасности в профессиональной деятельности» относится к базовой части учебного плана.

Дисциплина изучается на 4 курсе, в 8 семестре.

Для изучения дисциплины требуется: Для освоения дисциплины студенты используют знания, умения, навыки, способы деятельности и установки, полученные и сформированные в ходе изучения дисциплин «Информатика и информационные технологии в профессиональной деятельности».

Изучению дисциплины Б1.Б.09 «Основы информационной безопасности в профессиональной деятельности» предшествует освоение дисциплин (практик):

Б1.Б.08 Информатика и информационные технологии в профессиональной деятельности.

Освоение дисциплины Б1.Б.09 «Основы информационной безопасности в профессиональной деятельности» является необходимой основой для последующего изучения дисциплин (практик):

Б2.Б.02(П) Практика по получению профессиональных умений и опыта профессиональной деятельности.

Область профессиональной деятельности, на которую ориентирует дисциплина «Основы информационной безопасности в профессиональной деятельности», включает: межкультурную коммуникацию в сферах межгосударственных отношений, обеспечения обороны и безопасности государства, законности и правопорядка.

Освоение дисциплины готовит к работе со следующими объектами профессиональной деятельности:

- информация, передаваемая в процессе межкультурной коммуникации;
- иностранные языки и культуры;
- теория изучаемых иностранных языков и перевода;
- способы, методы, средства, виды и приемы межкультурной коммуникации в сферах межгосударственных отношений, обеспечения обороны и безопасности государства, законности и правопорядка;
- информационно-аналитическая, редакторская и организационная деятельность в области перевода.

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 компетенций.

Выпускник должен обладать следующими общепрофессиональными компетенциями (ОПК):

ОПК-1 способностью работать с различными источниками информации, информационными ресурсами и технологиями, осуществлять поиск, хранение, обработку и анализ информации из разных источников и баз данных, представлять её в требуемом формате с использованием информационных, компьютерных и сетевых технологий, владеть стандартными методами компьютерного набора текста и его редактирования на русском и иностранном языке.

ОПК-2 способностью соблюдать в профессиональной деятельности требования правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, обеспечивать соблюдение режима секретности.

ОПК-5 способностью самостоятельно осуществлять поиск профессиональной информации в печатных и электронных источниках, включая электронные базы данных.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Восьмой семестр
Контактная работа (всего)	**54**	**54**
Лекции	18	18
Практические	36	36
Самостоятельная работа (всего)	**54**	**54**
Виды промежуточной аттестации		
Зачет		+
Общая трудоемкость часы	**108**	**108**
Общая трудоемкость зачетные единицы	**3**	**3**

5. Содержание дисциплины

5.1. Содержание модулей дисциплины

Модуль 1. Основы информационную безопасность:

Общие вопросы информационной безопасности. Теория информационной безопасности и ее основные направления. Виды возможных нарушений информационной безопасности. Причины возникновения информационных угроз и меры защиты от них. Международные стандарты информационного обмена. Понятие информационной угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». Нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Закон об информации. Судебные прецеденты и ответственность за нарушение закона. Концепция информационной безопасности РФ. Информационная безопасность личности, общества, государства. Теория информационной безопасности и ее основные направления. Ведущие положения теории информационной безопасности в области информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

Виды возможных нарушений информационной безопасности. Несформированность информационной культуры пользователей. Хакерские атаки. DoS- и DDoS-атаки. Сетевой шпионаж (сниффинг, нюкеры). Эксплойты. Причины возникновения информационных угроз. Анализ способов нарушения информационной безопасности. Использование защищенных компьютерных систем. Назначение и задачи в сфере обеспечения инфор-мационной безопасности на уровне государства.

Информационные ресурсы по информационной безопасности. Правовые вопросы, связанные с информационной безопасностью. Нормативные руководящие документы, касающиеся государственной тайны.

Модуль 2. Современные технологии информационной безопасности:

Назначение и задачи обеспечения информационной безопасности на уровне государства. Понятие о видах вирусов. Антивирусная защита компьютера. Технология построения защищенных информационных систем. Криптография как наука. Методы психологического воздействия на пользователя сети Интернет. Понятие о видах вирусов. Антивирусная защита компьютера. Классификация компьютерных вирусов. Классические компьютерные вирусы. Файловые вирусы. Макровирусы. Троянские кони. Руткиты. Сетевые черви. Программные средства для обеспечения антивирусной защиты компьютера.

Технологии построения защищенных информаци-онных систем. Место информационной безопасности экономических систем в национальной без-опасности страны. Риски и ценность информации.

Криптография как наука. Методы криптографии. Алгоритмы и стандарты шифрования. Симметричное и асимметричное шифрование. Электронная цифровая подпись. Современные технологии аутентификации.

Вопросы организации информационной безопасности при работе с информационными ресурсами и сервисами сети Интернет. Методы психологического воздействия на пользователя сети Интернет. Социальная инженерия.

Антивирусные программные средства офисного и домашнего назначения для обеспечения информационной безопасности. Парольная защита. Программы шифрования данных

Социальная инженерия и ее методы.

Электронная валюта

Социальные сети как информационная угроза. Дети и Интернет. Политика информационной безопасности и ее организация в локальной сети

5.2. Содержание дисциплины: Лекции (18 ч.)

Модуль 1. Основы информационную безопасность (8 ч.)

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

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

Тема 2. Теория информационной безопасности и ее основные направления (2 ч.)

Теоретические вопросы организации информационной безопасности. Пути организации информационной безопасности на предприятии.

Тема 3. Виды возможных нарушений информационной безопасности (2 ч.)

Информационная угроза. Уровни нарушения информационной безопасности: аппаратный, программный, человеческий фактор.

Тема 4. Причины возникновения информационных угроз и меры защиты от них (2 ч.)

Информационная угроза. Виды информационных угроз. Способы защиты от информационных угроз.

Модуль 2. Современные технологии информационной безопасности (10 ч.)

Тема 5. 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.

Тема 6. 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 7. 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 8. Криптография как наука (2 ч.)

Криптография и ее место в обеспечении информационной безопасности предприятия. Способы шифрования данных. Программы для шифровки и расшифровки данных.

Тема 9. Программные средства компьютера по обнаружению несанкционированного вторжения и защите от вторжения (2 ч.)

Психологическое воздействия на пользователя как информационная угроза. Способы воздействия. Психологическое воздействие. Способы защиты от воздействия.

5.3. Содержание дисциплины: Практические (36 ч.)

Модуль 1. Основы информационную безопасность (18 ч.)

Тема 1. Информационные ресурсы по информационной безопасности (2 ч.)

Общие вопросы информационной безопасности. Информационные ресурсы по информационной безопасности.

Тема 2. 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 3. Правовые вопросы, связанные с информационной безопасностью (2 ч.)

Интеллектуальная собственность. Способы защиты интеллектуальной собственности.

Лицензионное программное обеспечение. Компьютерное пиратство и законодательная ответственность за него.

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

Государственная тайна. Ответственность за разглашение государственной тайны.

Состояние законодательства РФ в области сохранения государственной тайны.

Примеры нарушения государственной тайны.

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. Ограничение доступа к USB-накопителям. Разграничение доступа в локальных сетях. Взлом учетных записей пользователей локальной сети. Способы предотвращения взлома.

Тема 6. 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 7. Комплексная защита сетевого компьютера от информационных угроз (2 ч.)

Проблемы выбора защитного программного обеспечения. Сайты с бесплатным программным обеспечением по защите компьютера.

Хакинг и антихакинг. Хакерские технологии.

Обзор программных средств для защиты объектов операционной системы.

Тема 8. Брандмауэр как аппаратное и программное средство ограничения доступа к информации (2 ч.)

Брандмауэр (межсетевой экран, firewall) и его назначение. Технология отражения атак брандмауэром. Настройка встроенного брандмауэра Windows.

Характеристики специализированных брандмауэров. Критерии отбора брандмауэров для практического использования.

Тема 9. 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.

Модуль 2. Современные технологии информационной безопасности (18 ч.)

Тема 10. Антивирусные программные средства офисного и домашнего назначения (2 ч.)

Вредоносное программное обеспечение и пути его попадания в компьютер пользователя.

Компьютерная реклама как инструмент заражения компьютера. Руткиты.

Клавиатурные шпионы (кейлоггеры). Функциональные возможности антивирусных программных средств.

Онлайн антивирусы

Sms-блокеры и методы борьбы с ними.

Тема 11. Парольная защита (2 ч.)

Пароль как средство ограничения доступа к ресурсу. Требования к выбору пароля. Хранители паролей.

Программы восстановления (взлома) паролей. Брутфорс

Тема 12. 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 13. 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 14. Программы шифрования данных (2 ч.)

Шифрование данных и его назначение. Алгоритмы и стандарты шифрования. Архивирование файлов с паролем как инструмент защиты от несанкционированного

доступа.

Криптография и ее методы шифрования информации. Восстановление данных. Грамотное удаление информации с компьютера. Специализированные программные средства по удалению.

Тема 15. Электронная валюта (2 ч.)

Электронная наличность. Обзор платежных онлайн-систем. Опасности при работе с электронной наличностью.

Проблемы электронной оплаты.

Способы заработка в Интернете.

Тема 16. 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 17. Фильтрация сетевого контента (2 ч.)

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

Тема 18. 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.

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

6.1 Вопросы и задания для самостоятельной работы

Восьмой семестр (54 ч.)

Модуль 1. Основы информационную безопасность (27 ч.)

Вид СРС: *Выполнение индивидуальных заданий

Подготовка ситуационных задач по информационной безопасности на основании статей соответствующих 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 по договору

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

следования

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 смежных прав

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 передачи компьютерной 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, органами государственной 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 государственной тайне

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 ранее допускавшихся 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 нормативных актов, на которые осуществлялась опора.

Пример задачи:

Гражданин Иванов создал антивирусное программное средство под названием «EFVIv»

и 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 гражданина Иванова?

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:

2) 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: *Работа с электронными ресурсами и информационными системами

Прохождение онлайн курса:

"Технологии и продукты Microsoft в обеспечении информационной безопасности " http://www.intuit.ru/studies/courses/600/456/info.

Модуль 2. Современные технологии информационной безопасности (27 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 информацион-ной безопасности на компьютере

Список приложений для рассмотрения

Межсетевые экраны (со встроенным и без встроенного антивируса)

AVG Internet Security

ViPNet Personal Firewall

BitDefender Total Security

Norton Internet Security

F-Secure Internet Security
Antiy GhostBusters
eScan Internet Security Suite
Agnitum Outpost Firewall Pro
Jetico Personal Firewall
Core Force
Privatefirewall
PC Tools Firewall Plus
Программы проактивной защиты и защиты от шпионских программ
WinPatrol
Ad-Aware
SUPERAntiSpyware
Spyware Doctor
AVZ
Windows Defender
Spybot - Search & Destroy
Spyware Terminator
HijackThis
Spy Sweeper
SpywareBlaster
Системы обнаружения вторжения
Anti-keylogger
Protector Plus
Можно выбрать свои программные средства, не указанные выше.
Вид СРС: *Работа с электронными ресурсами и информационными системами

Прохождение онлайн курса:
"Основы информационной безопасности при работе на компьютере" http://www.intuit.ru/studies/courses/680/536/info

7. Тематика курсовых работ(проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

8. Фонд оценочных средств для промежуточной аттестации

8.1. Компетенции и этапы формирования

Коды компетенций	Этапы формирования		
	Курс, семестр	Форма контроля	Модули (разделы) дисциплины
ОПК-2	4 курс, Восьмой семестр	Зачет	Модуль 1: Основы информационную безопасность.
ОПК-1 ОПК-5	4 курс, Восьмой семестр	Зачет	Модуль 2: Современные технологии информационной безопасности.

Сведения об иных дисциплинах, участвующих в формировании данных компетенций:
Компетенция ОПК-1 формируется в процессе изучения дисциплин:
Информатика и информационные технологии в профессиональной деятельности, Научно-исследовательская работа, Основы информационной безопасности в профессиональной деятельности, Практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской

деятельности, Практика по получению профессиональных умений и опыта профессиональной деятельности.

Компетенция ОПК-2 формируется в процессе изучения дисциплин:

Безопасность жизнедеятельности, Основы информационной безопасности в профессиональной деятельности, Правовые основы деятельности переводчика, Практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности, Практика по получению профессиональных умений и опыта профессиональной деятельности.

Компетенция ОПК-5 формируется в процессе изучения дисциплин:

Информатика и информационные технологии в профессиональной деятельности, Научно-исследовательская работа, Основы информационной безопасности в профессиональной деятельности, Практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности, Практика по получению профессиональных умений и опыта профессиональной деятельности, Практический курс перевода второго иностранного языка, Практический курс перевода первого иностранного языка, Преддипломная практика, Теория межкультурной коммуникации.

8.2. Показатели и критерии оценивания компетенций, шкалы оценивания

В рамках изучаемой дисциплины студент демонстрирует уровни овладения компетенциями:

Повышенный уровень:

знает и понимает теоретическое содержание дисциплины; творчески использует ресурсы (технологии, средства) для решения профессиональных задач; владеет навыками решения практических задач.

Базовый уровень:

знает и понимает теоретическое содержание; в достаточной степени сформированы умения применять на практике и переносить из одной научной области в другую теоретические знания; умения и навыки демонстрируются в учебной и практической деятельности; имеет навыки оценивания собственных достижений; умеет определять проблемы и потребности в конкретной области профессиональной деятельности.

Пороговый уровень:

понимает теоретическое содержание; имеет представление о проблемах, процессах, явлениях; знаком с терминологией, сущностью, характеристиками изучаемых явлений; демонстрирует практические умения применения знаний в конкретных ситуациях профессиональной деятельности.

Уровень ниже порогового:

имеются пробелы в знаниях основного учебно-программного материала, студент допускает принципиальные ошибки в выполнении предусмотренных программой заданий, не способен продолжить обучение или приступить к профессиональной деятельности по окончании вуза без дополнительных занятий по соответствующей дисциплине.

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%

Критерии оценки знаний студентов по дисциплине

Оценка	Показатели
Зачтено	Владееет навыками организации информационной безопасности на компьютере
Незачтено	Не владееет навыками организации информационной безопасности на компьютере

8.3. Вопросы, задания текущего контроля

Модуль 1: Основы информационную безопасность

ОПК-2 способность соблюдать в профессиональной деятельности требования правовых актов в области информационной безопасности, защиты государственной тайны и иной информации ограниченного доступа, обеспечивать соблюдение режима секретности

1. Раскройте суть нормативно-правового аспекта защиты информации. Охарактеризуйте структуру законодательства России в области защиты информации.

2. Дайте определение государственной тайне. Перечислите основные статьи в Законе о государственной тайне.

3. Дайте определение понятиям «авторское право» и «коммерческая тайна». Укажите их отличительные особенности. Охарактеризуйте способы защиты авторских прав и коммерческой тайны.

4. Перечислите виды конфиденциальной информации. Приведите примеры конфиденциальной информации и укажите способы ее защиты.

5. Перечислите нормативно-правовые документы, ориентированные на обеспечение информационной безопасности. Охарактеризуйте нарушения, представленные в этих документах и меру наказания.

Модуль 2: Современные технологии информационной безопасности

ОПК-1 способность работать с различными источниками информации, информационными ресурсами и технологиями, осуществлять поиск, хранение, обработку и анализ информации из разных источников и баз данных, представлять её в требуемом формате с использованием информационных, компьютерных и сетевых технологий, владеть стандартными методами компьютерного набора текста и его редактирования на русском и иностранном языке

1. Раскройте понятие «компьютерный вирус». Перечислите виды компьютерных вирусов. Приведите примеры, опишите способы их проникновения и особенности разрушительных действий.

2. Перечислите способы проникновения компьютерных вирусов на компьютер. Приведите примеры, опишите особенности их разрушительных действий.

3. Раскройте суть технология антивирусной защиты сетевого компьютера. Приведите примеры антивирусных приложений и укажите особенности их функционала.

4. Охарактеризуйте вредоносные программы и их виды. Перечислите способы борьбы с ними.

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

ОПК-5 способность самостоятельно осуществлять поиск профессиональной информации в печатных и электронных источниках, включая электронные базы данных

1. Укажите виды мошенничества в сети Интернет. Перечислите способы противодействия Интернет-мошенникам. Охарактеризуйте поведение при возникновении угрозы Интернет-мошенников.

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

3. Сформулируйте рекомендации для обеспечения безопасности в приложениях MS Word и MS Excel. Опишите способы защиты информации в БД на примере MS Access.

4. Раскройте суть идентификация и аутентификация при входе в информационную

систему. Сформулируйте рекомендации по использованию парольных схем в компьютерных сетях. Укажите недостатки парольных схем.

5. Раскройте технологию функционирования брандмауэров. Объясните настройку брандмауэра на примере конкретного приложения.

8.4. Вопросы промежутосной аттестации

Восьмой семестр (Зачет, ОПК-1, ОПК-2, ОПК-5)

1. Раскройте различные подходы к определению понятия «информационная безопасность». Привести примеры нарушения информационной безопасности в быту и на предприятии.

2. Обоснуйте этапы развития информационной безопасности.

3. Раскройте понятие «защита информации» и обоснуйте основные аспекты защиты информации.

4. Обоснуйте основные задачи системы информационной безопасности.

5. Охарактеризуйте программные средства организации информационной безопасности при работе на компьютере. На примере одного приложения раскройте его функциональные возможности по защите информации.

6. Охарактеризуйте программные средства организации информационной безопасности в компьютерной сети. На примере одного приложения раскройте его функциональные возможности по защите информации.

7. Охарактеризуйте аппаратные средства организации информационной безопасности при работе на компьютере. Приведите примеры аппаратных средств защиты информации.

8. Укажите основные направления организации информационной безопасности. Сформулируйте рекомендации для организации информационной безопасности при работе на ПК для сотрудников образовательного учреждения.

9. Раскройте понятие «сетевые атаки». Приведите примеры сетевых атак. Укажите способы несанкционированного проникновения на сетевой компьютер и охарактеризуйте пути противодействия им.

10. Раскройте понятие «информационная угроза» с позиции проблемы обеспечения информационной безопасности. Охарактеризуйте виды угроз. Приведите примеры угроз различных видов.

11. Раскройте суть нормативно-правового аспекта защиты информации. Охарактеризуйте структуру законодательства России в области защиты информации.

12. Дайте определение государственной тайне. Перечислите основные статьи в Законе о государственной тайне.

13. Дайте определение понятиям «авторское право» и «коммерческая тайна». Укажите их отличительные особенности. Охарактеризуйте способы защиты авторских прав и коммерческой тайны.

14. Перечислите виды конфиденциальной информации. Приведите примеры конфиденциальной информации и укажите способы ее защиты.

15. Перечислите нормативно-правовые документы, ориентированные на обеспечение информационной безопасности. Охарактеризуйте нарушения, представленные в этих документах и меру наказания.

16. Охарактеризуйте организационные меры защиты информации. Обоснуйте основные организационные мероприятия информационной безопасности.

17. Охарактеризуйте технологические меры информационной безопасности. Обоснуйте классификацию средств технологической защиты информации.

18. Охарактеризуйте аппаратные средства защиты информации, укажите основания для их классификации. Приведите примеры аппаратных средств защиты информации.

19. Опишите суть программной защиты информации. Перечислите основные средства программной защиты информации, обоснуйте их классификацию. На примере одного приложения раскройте его функциональные возможности по защите информации.

20. Перечислите антивирусные программные средства. На примере конкретного приложения продемонстрируйте настройку безопасности.

21. Раскройте понятие «компьютерный вирус». Перечислите виды компьютерных вирусов. Приведите примеры, опишите способы их проникновения и особенности разрушительных действий.

22. Перечислите способы проникновения компьютерных вирусов на компьютер. Приведите примеры, опишите особенности их разрушительных действий.

23. Раскройте суть технология антивирусной защиты сетевого компьютера. Приведите примеры антивирусных приложений и укажите особенности их функционала.

24. Охарактеризуйте вредоносные программы и их виды. Перечислите способы борьбы с ними.

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

26. Укажите виды мошенничества в сети Интернет. Перечислите способы противодействия Интернет-мошенникам. Охарактеризуйте поведение при возникновении угрозы Интернет-мошенников.

27. Раскройте цели и задач криптографии как научной области. Перечислите основные направления использования криптографических методов.

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

29. Охарактеризуйте методы криптографического закрытия информации. Опишите суть стойкости метода и трудоемкости метода.

30. Охарактеризуйте современные способы шифрования данных.

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

32. Раскройте особенность парольной защиты информации. Укажите достоинства и недостатки парольной защиты информации. Назовите примеры программных средств для создания и хранения паролей.

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

34. Сформулируйте рекомендации для обеспечения безопасности в приложениях MS Word и MS Excel. Опишите способы защиты информации в БД на примере MS Access.

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

36. Раскройте технологию функционирования брандмауэров. Объясните настройку брандмауэра на примере конкретного приложения.

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

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.

При балльно-рейтинговом контроле знаний итоговая оценка выставляется с учетом набранной суммы баллов.

Собеседование (устный ответ) на зачете

Для оценки сформированности компетенции посредством собеседования (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.

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.

Контекстная учебная задача, проблемная ситуация, ситуационная задача, кейсовое задание

При определении уровня достижений студентов при решении учебных практических задач необходимо обращать особое внимание на следующее:

– способность определять и принимать цели учебной задачи, самостоятельно и творчески планировать ее решение как в типичной, так и в нестандартной ситуации;

– систематизированные, глубокие и полные знания по всем разделам программы;

– точное использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы и задания;

– владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении учебных задач;

– грамотное использование основной и дополнительной литературы;

– умение использовать современные информационные технологии для решения учебных задач, использовать научные достижения других дисциплин;

– творческая самостоятельная работа на практических, лабораторных занятиях, активное участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

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

2. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс] : учебное пособие / Ю. Н. Загинайлов. – М. ; Берлин : Директ-Медиа, 2015. – 253 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=276557

3. Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С. А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. – СПб. :

Издательство Политехнического университета, 2014. – 322 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=363040

4. Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О. В. Прохорова. – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=438331

Дополнительная литература

1. Сычев, Ю. Н. Основы информационной безопасности. Учебн [Электронный ресурс] : практическое пособие / Ю. Н. Сычев. - М.: Евразийский открытый институт, 2010. - 328 с. - 978-5-374-00381-9. Режим доступа : http://biblioclub.ru/index.php?page=book&id=90790.

2. Конституция Российской Федерации.

3. ФЗ РФ «Об информации, информатизации и защите информации».

4. ФЗ РФ "О персональных данных"

5. ФЗ РФ «О безопасности».

6. ФЗ РФ «О государственной тайне».

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://www.securrity.ru - SecuRRity.Ru — «Информационная безопасность компьютерных систем и защита конфиденциальных данных»

2. http://all-ib.ru - Информационная безопасность. Защита информации

3. http://www.securitylab.ru - Security Lab by Positive Technologies [Электронный ресурс] . – URL: http://www.securitylab.ru

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 лекционному материалу, а затем по другим источникам;

– прочитайте дополнительную литературу из списка, предложенного преподавателем;

– выпишите в тетрадь основные категории и персоналии по теме, используя лекционный материал или словари, что поможет быстро повторить материал при подготовке к зачету;

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

– выучите определения терминов, относящихся к теме;

– продумайте примеры и иллюстрации к ответу по изучаемой теме;

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

– продумывайте высказывания по темам, предложенным к лабораторному занятию.

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 на карточках, что поможет

при подготовке рефератов, текстов речей, при подготовке к зачету;

– 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

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

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 студентами фиксируются в электронной информационно-образовательной среде университета.

Учебная аудитория для проведения лекционных занятий, практических (семинарских) занятий.

Компьютерный класс (№111).

Помещение укомплектовано специализированной учебной мебелью и техническими средствами обучения.

Основное оборудование:

Наборы демонстрационного оборудования: автоматизированное рабочее место преподавателя в составе (системный блок, монитор, фильтр, мышь, клавиатура, веб камера, документ камера, акустическая система), проектор, интерактивная доска.

Автоматизированные рабочие места в составе (компьютеры – 13 штук), магнитола JVC RD-EZ16, магнитно-маркерная доска.

Учебно-наглядные пособия:

Презентации, учебные плакаты.

Помещение для самостоятельной работы, № 114

Помещение укомплектовано специализированной учебной мебелью и техническими средствами обучения.

Основное оборудование:

Автоматизированное рабочее место в составе (системный блок, монитор, фильтр, мышь, клавиатура, веб камера) с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета; телевизор LG.

Учебно-наглядные пособия:

Презентации, учебные плакаты.

Помещение для самостоятельной работы.

Читальный зал электронных ресурсов, №101б

Помещение укомплектовано специализированной учебной мебелью и техническими средствами обучения.

Основное оборудование:

Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета автоматизированные рабочие места (компьютер – 12 штук).

Мультимедийный проектор, многофункциональное устройство, принтер.

Учебно-наглядные пособия:

Презентации, электронные диски с учебными и учебно-методическими пособиями.

Помещение для самостоятельной работы.

Читальный зал, № 101

Помещение укомплектовано специализированной учебной мебелью и техническими средствами обучения.

Основное оборудование:

Компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета: автоматизированные рабочие места (компьютер – 10 штук).

Проектор с экраном, многофункциональное устройство, принтер.

Учебно-наглядные пособия:

Учебники и учебно-методические пособия, периодические издания, справочная литература, стенды с тематическими выставками.