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

Факультет естественно-технологический
Кафедра информатики и вычислительной техники

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Наименование дисциплины (модуля): Основы защиты информации в компьютерных сетях
Уровень ОПОП: Бакалавриат

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

Разработчики:
Зубрилин А. А., канд. филос. наук, доцент
Лапин К. С., канд. физ.-мат. наук, доцент
Харитонова А. А., канд. пед. наук, доцент

Программа рассмотрена и утверждена на заседании кафедры, протокол № 11 от 18.05.2017 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.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины - формирование педагога, способного организовывать безопасную работу на персональном компьютере и в компьютерной сети, умеющего противостоять информационным угрозам, включая технические, технологические, психологические, социальные; способного использовать естественнонаучные и математические знания для реализации образовательных программ по информатике и использовать возможности образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса.

Задачи дисциплины:

- формирование знаний в области российского правового регулирования информационной безопасности для реализации образовательных программ по информатике;
- выработка представлений о способах обеспечения защиты компьютера и противостоянии методам социальной инженерии с использованием естественнонаучных и математических знаний м целью реализации образовательных программ по информатике.
- 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 с использованием возможностей образовательной среды с целью реализации образовательных программ по информатике;
- обучение основам криптографии, как одного из важных средств шифрования данных для реализации образовательных программ по информатике.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина Б1.В.ДВ.17.1 «Основы защиты информации в компьютерных сетях» относится к вариативной части учебного плана.

Дисциплина изучается на 4 курсе, в 8 семестре.

Для изучения дисциплины требуется: знание возможностей сервисов сети Интернет

Изучению дисциплины Б1.В.ДВ.17.01 «Основы защиты информации в компьютерных сетях» предшествует освоение дисциплин (практик):

Информационные технологии в образовании;

Проектирование информационно-образовательной среды.

Освоение дисциплины Б1.В.ДВ.17.01 «Основы защиты информации в компьютерных сетях» является необходимой основой для последующего изучения дисциплин (практик):

Администрирование компьютерных сетей.

Область профессиональной деятельности, на которую ориентирует дисциплина «Основы защиты информации в компьютерных сетях», включает: образование, социальную сферу, культуру.

Освоение дисциплины готовит к работе со следующими объектами профессиональной деятельности:

- обучение;
- воспитание;
- развитие.

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 и трудовых функций (профессиональный стандарт Педагог (педагогическая деятельность в дошкольном, начальном общем, основном общем, среднем общем образовании) (воспитатель, учитель), утвержден приказом Министерства труда и социальной защиты №544н от 18.10.2013).

Выпускник должен обладать следующими профессиональными компетенциями (ПК) в соответствии с видами деятельности:

ПК-1. готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов

педагогическая деятельность

ПК-1 готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов	знать: - понятия, связанные с научной областью «Информационная безопасность» с целью реализации образовательных программ по информатике; - возможные технические, технологические, социальные угрозы, связанные с компьютерной техникой с целью реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов; - меры соблюдения информационной безопасности при работе на компьютере в условиях реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов; - виды информационных угроз, возникающих при работе в компьютерных сетях с целью реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов; - программные средства и сервисы Интернет для обеспечения информационной безопасности с целью реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов; - способы шифрования данных для реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов; - правовые и законодательные акты в области обеспечения информационной безопасности для реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов; уметь: - аргументировано выбирать и эффективно использовать программные средства для обеспечения информационной безопасности в условиях реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов; - определять оптимальный набор программных средств для обеспечения безопасной работы на компьютере; владеть: - средствами обеспечения информационной безопасности при работе за персональным компьютером и в компьютерных сетях в условиях реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Восьмой семестр
Контактная работа (всего)	**26**	**26**
Практические	26	26
Самостоятельная работа (всего)	**46**	**46**
Виды промежуточной аттестации		
Зачет		+
Общая трудоемкость часы	**72**	**72**
Общая трудоемкость зачетные единицы	**2**	**2**

5. Содержание дисциплины

5.1. Содержание модулей дисциплины

Модуль 1. Проблемы информационной безопасности в современном обществе:

Информационные ресурсы по информационной безопасности. Правовые вопросы, связанные с информационной безопасностью. Правовые впоросы, связанные с информационной безопасностью. Нормативные документы, касающиеся государственной тайны. Программные и аппаратные средства, связанные с угрозой обеспечения информационной безопасности. DoS- и DDoS-атаки как инструмент ограничения доступа к сетевому ресурсу.

Модуль 2. Практические вопросы организации информационной безопасности в компьютерных сетях:

Комплексная защита сетевого компьютера от информационных угроз. Брандмауэр как аппаратное и программное средство ограничения доступа к информации. Программные средства компьютера по обнаружению несанкционированного вторжения и защите от вторжения. Антивирусные программные средства офисного и домашнего назначения.

Парольная защита. Социальная инженерия и ее методы.

5.2. Содержание дисциплины: Практические (26 ч.)

Модуль 1. Проблемы информационной безопасности в современном обществе (12 ч.)

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

Обзор информационных ресурсов по информационной безопасности. Направления организации информационной безопасности в компьютерных сетях.

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.

Модуль 2. Практические вопросы организации информационной безопасности в компьютерных сетях (14 ч.)

Тема 7. Комплексная защита сетевого компьютера от информационных угроз (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 8. Брандмауэр как аппаратное и программное средство ограничения доступа к информации (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 инфор-мационными ресурсами.

Тема 9. Программные средства компьютера по обнаружению несанкционированного вторжения и защите от вторжения (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 10. Антивирусные программные средства офисного и домашнего назначения (2 ч.)

Проблемы выбора защитного программного обеспечения. Сайты с бес-платным программным обеспечением по защите компьютера. Хакинг и антихакинг. Хакерские технологии. Обзор программных средств для защиты объектов операционной системы.

Тема 11. Парольная защита (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 12. Социальная инженерия и ее методы (2 ч.)

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

Тема 13. Социальная инженерия и ее методы (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.

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

6.1 Вопросы и задания для самостоятельной работы

Восьмой семестр (46 ч.)

Модуль 1. Проблемы информационной безопасности в современном обществе (24 ч.)

Вид СРС: *Выполнение компетентностно-ориентированных 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.

Модуль 2. Практические вопросы организации информационной безопасности в компьютерных сетях (22 ч.)

Вид СРС: *Выполнение индивидуальных заданий

Дайте развернутый письменный ответ на следующие вопросы.

Информационная безопасность в социальных сетях

1. На примере известных социальных сетей приведите примеры несанкционированного доступа к личной информации и опишите, как этого можно было бы избежать.(20 баллов)

2. На примере известных социальных сетей опишите, как настройки приватности влияют на информационную безопасность Вашего аккаунта. (20 баллов)

3. Подготовьте документы Microsoft Word и Microsoft Excel, защищенные от несанкционированного доступа. (20 баллов)

4. Приведите три различных примера мошенничества в интернете (по возможности добавьте ссылку на данную информацию). (20 баллов)

5. Опишите, какие способы доступа к конфиденциальной информации используются в международных компаниях (20 баллов)

7. Тематика курсовых работ(проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

8. Оценочные средства для промежуточной аттестации

8.1. Компетенции и этапы формирования

Коды компетенций	Этапы формирования		
	Курс, семестр	Форма контроля	Модули (разделы) дисциплины
ПК-1	4 курс, Восьмой семестр	Зачет	Модуль 1: Проблемы информационной безопасности в современном обществе.
ПК-1	4 курс, Восьмой семестр	Зачет	Модуль 2: Практические вопросы организации информационной безопасности в компьютерных сетях.

Сведения об иных дисциплинах, участвующих в формировании данных компетенций:
Компетенция ПК-1 формируется в процессе изучения дисциплин:
3D моделирование, Администрирование компьютерных сетей, Биотехнологические производства Республики Мордовия, Инженерная графика в технологическом образовании, Информационная безопасность в образовании, Информационные системы, История и методология информатики и вычислительной техники, Компьютерное моделирование, Математика, Математические методы в конструировании, Методика обучения информатике, Методика обучения технологии, Метрология и техническое законодательство, Обустройство и дизайн дома, Организация и технология предприятий бытового обслуживания, Основы конструирования, Основы материаловедения и технологии обработки материалов, Основы микроэлектроники, Основы моделирования в швейном производстве, Основы моделирования машин и механизмов, Основы нанотехнологий, Основы рационального природопользования, Основы сельского хозяйства, Основы теории машин и механизмов, Основы теории технологической подготовки, Практикум по информационным технологиям, Практикум по кулинарии, Практикум по швейному производству, Программирование, Проектирование в системах автоматизированного проектирования, Разработка приложений в Microsoft Visual Studio, Разработка электронных образовательных ресурсов и методика их оценки, Свободные инструментальные системы, Современные проблемы биотехнологии, Социальная экология, Специальное рисование, Стандартизация и сертификация в современном производстве, Теория графов в информатике, Техническое черчение, Технологии обработки металла и дерева, Технологии переработки сельскохозяйственной продукции, Технологии современных производств, Технология обработки ткани и пищевых продуктов, Физика, Химические производства Республики Мордовия, Химический мониторинг состояния окружающей среды, Химия, Химия в пищевой промышленности, Химия в текстильной промышленности, Экологический мониторинг состояния окружающей среды, Электротехнические и радиотехнические устройства.

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
	Зачет	
Повышенный	зачтено	90 – 100%
Базовый	зачтено	76 – 89%
Пороговый	зачтено	60 – 75%
Ниже порогового	незачтено	Ниже 60%

Критерии оценки знаний студентов по дисциплине

Оценка	Показатели
Зачтено	Студент владеет навыками организации информационной безопасности на компьютере
Незачтено	Студент не владеет навыками организации информационной безопасности на компьютере

8.3. Вопросы, задания текущего контроля

Модуль 1: Проблемы информационной безопасности в современном обществе

ПК-1 готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов

1. Опишите процедуру установки на компьютер антивирусного программеого средства (из списка)

Модуль 2: Практические вопросы организации информационной безопасности в компьютерных сетях

ПК-1 готовностью реализовывать образовательные программы по учебным предметам в соответствии с требованиями образовательных стандартов

1. Каким способами можно избежать негативного влияния сети интернет на ваш нерсональный компьютер?

8.4. Вопросы промежуточной аттестации

Восьмой семестр (Зачет, ПК-1)

1. Раскройте понятие «информационная безопасность». Приведите примеры нарушения информационной безопасности в быту и на предприятии.
2. Расскажите о программных средствах организации информационной безопасности при работе на компьютере и в компьютерной сети.
3. Расскажите об аппартных средствах организации информационной безопасности при работе на компьютере и в компьютерной сети.
4. Раскройте основные направления организации информационной безопасности.
5. Приведите способы несанкционированного проникновения на сетевой компьютер и пути противодействия им
6. Раскройте понятие «информационная угроза» с позиции проблемы обеспечения информационной безопасности
7. Дайте понятие административным, государственным и правовым вопросам, регламентирующим деятельность по организации информационной безопасности
8. Опишите технологию функционирования брандмауэров. Объяснить настройку брандмауэра на примере конкретного приложения
9. Опишите технологию функционирования антивирусных программных средств. Объясните настройку антивируса на примере конкретного приложе-ния
10. Раскройте понятие «компьютерный вирус». Описать виды компьютерных вирусов, способы их проникновения на компьютер.
11. Раскройте технологию антивирусной защиты сетевого компьютера
12. Дайте понятие криптографии как научной области, связанной с шифрованием данных
13. Опишите способы шифрования данных
14. Опишите программные средства шифрования данных. Объясните технологию шифрования на примере конкретного приложения
15. Опишите на примере конкретного приложения технологию функционирования программных средств, использующихся для создания и хранения паролей
16. Опишите принципы организации DoS- и DoSS-атак. Приведите способы борьбы с данным видом информационной угрозы
17. Дайте понятие политики информационной безопасности. Опишите способы организации политики информационной безопасности на предприятии
18. Раскройте сущность потенциально опасных программ. Опишите способы борьбы с ними
19. Расскажите о системах отражения сетевых атак. Опишите их виды, принципы функционирования
20. Расскажите о проактивных системах защиты компьютера. Приведите примеры программ данного класса
21. Расскажите о системах контроля целостности. Приведите примеры программ данного класса
22. Расскажите о спаме как не затребованной Интернет-рекламе. Приведите способы борьбы со спамом
23. Расскажите о программах ограничения доступа в Интернет и фильтрации информационных ресурсов
24. Опишите социальные сети как инструмент сбора информации о пользователей
25. Дайте понятие хакинга. Приведите характеристику хакеру как лицу, пытающемуся незаконно завладеть конфиденциальной информацией

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

Промежуточная аттестация проводится в форме зачета.

Зачет позволяет оценить сформированность компетенций, теоретическую подготовку студента, его способность к творческому мышлению, готовность к практической деятельности, приобретенные навыки самостоятельной работы, умение синтезировать

полученные знания и применять их при решении практических задач.

При балльно-рейтинговом контроле знаний 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.

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. 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 ://biblioclub.ru/index.php?page=book&id=276557

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

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 ://biblioclub.ru/index.php?page=book&id=363040

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

5. Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях [Электронный ресурс]: учебное пособие / М. А. Иванов, И. В. Чугунков ; под ред. М. А. Иванова ; Министерство образования и науки Российской Федерации, Национальный исследовательский ядерный университет «МИФИ». – М. : МИФИ, 2012. – 400 с. –Режим доступа :http://biblioclub.ru/index.php?page=book&id=231673

6. 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

Дополнительная литература

1. Комарова, Е. С. Практикум по программированию на языке Паскаль [Электронный ресурс] : учебное пособие / Е. С. Комарова. – Москва ; Берлин : Директ-Медиа, 2015. – Ч. 1. – 85 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=426942

10. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://edu-top.ru/katalog - Университетская библиотека онлайн [Электронный ресурс]. – М. : Издательство «Директ-Медиа». – Режим доступа: http://biblioclub.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 по теме, используя лекционный материал или дополнительные источники, 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 к ответу по изучаемой теме.

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

(обновление призводится по мере появления новых версий программы)

1. Microsoft Windows 7 Pro

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

12.2 Перечень информационных справочных систем
(обновление выполняется еженедельно)

1. 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. Научная электронная библиотека e-library(http://www.e-library.ru/)

13. Материально-техническое обеспечение дисциплины(модуля)

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

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

Реализация учебной программы обеспечивается доступом каждого студента к информационным ресурсам – электронной библиотеке и сетевым ресурсам Интернет. Для использования ИКТ в учебном процессе необходимо наличие программного обеспечения, позволяющего осуществлять поиск информации в сети Интернет, систематизацию, анализ и презентацию информации, экспорт информации на цифровые носители.

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, курсового проектирования (выполнения курсовых работ), № 14.

Помещение укомплектовано специализированной мебелью и техническими средствами обучения.

Основное оборудование:

Наборы демонстрационного оборудования: автоматизированное рабочее место в составе (системный блок, монитор, клавиатура, мышь, гарнитура); интерактивная система информации; AverVision F55 (документ-камера).

Учебно-наглядные пособия:

Презентации.

Помещение для самостоятельной работы.

Читальный зал электронных ресурсов, № 101 б.

Помещение укомплектовано специализированной мебелью и техническими средствами обучения.

Основное оборудование:

Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета (компьютер 12 шт., мультимедийны проектор 1 шт., многофункциональное устройство 1 шт., принтер 1 шт.).

Учебно-наглядные пособия:

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