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

Физико-математический факультет

Кафедра Информатики и вычислительной техники

РАБОЧАЯПРОГРАММАДИСЦИПЛИНЫ
Информационная безопасность в образовании

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

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

Программа рассмотрена и утверждена на заседании кафедры, протокол № 9 от 15.04.2021 года

Зав. кафедрой _____ Зубрилин А. А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины – изучение основ информационной безопасности, формирование у студентов информационного мировоззрения на основе знания аспектов защиты информации; воспитание информационной культуры для эффективного применения полученных знаний в профессиональной деятельности.

Задачи дисциплины:

- изучение основных направлений организации информационной безопасности (правового, технического, аппаратного);
- изучение основ правового регулирования информационной безопасности в России в сфере образования;
- формирование знаний о технических способах и средствах обеспечения защиты информации в образовательных организациях;
- изучение программных средств обеспечения информационной безопасности при работе на ПК и в сети Интернет в образовательной организации;
- формирование умений аргументированного выбора и самостоятельной установки соответствующего программного обеспечения по защите данных на ПК;
- формирование умений разрабатывать и реализовывать политику информационной безопасности на предприятии, в частности в образовательном учреждении.

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.ДВ.02.2 «Информационная безопасность в образовании» относится к части учебного плана, формируемой участниками образовательных отношений.

Дисциплина изучается на 5 курсе, в 9 и 10 семестрах.

Для изучения дисциплины требуется: знание возможностей сервисов сети Интернет.

Изучению дисциплины «Защита информации в компьютерных сетях» предшествует освоение дисциплин (практик):

Информационные технологии в образовании.

Освоение дисциплины «Защита информации в компьютерных сетях» является необходимой основой для последующего изучения дисциплин (практик):

Информационная безопасность в образовании.

Область профессиональной деятельности, на которую ориентирует дисциплина «Защита информации в компьютерных сетях», 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 ирешения 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 задач в предметной области в соответствии с профилем и уровнем обучения и в области образования.	знать: - основные аспекты организации информационной безопасности в образовательных организациях; - нормативно-правовые основы информационной безопасности; - понятия информационной безопасности, изучаемые в школьном курсе информатики; уметь: - организовывать учебную деятельность для овладения способами защиты информации, изучаемые в школьном курсеинформатики; - проектировать политику информационной безопасности в условиях определенной образовательной организации; владеть: - методами, средствами и формами организации информационной безопасности в соответствии с принятыми правовыми нормами РФ;- подходами к формированию умений использовать современные методы защиты информации.
ПК-11.2 Проектирует и решает исследовательские задачи в предметной области в соответствии с профилем и уровнем обучения и в области образования.	знать: - способы организации информационной безопасности, изучаемых в школьном курсе информатики; уметь: - определять оптимальный набор программных средств для обеспечения безопасной работы на ПК; - применять способы защиты информации в компьютерных сетях; владеть: - методами организации комплексной защиты информациираз личного вида; - методами защиты конфиденциальной информации в условиях образовательной организации.
ПК-14. Способен устанавливать содержательные, методологические и мировоззренческиесвязи предметной области (в соответствии с профилем и уровнем обучения) со смежными научными областями.	
педагогическая деятельность	
ПК-14.4 Формирует междисциплинарные связи методики обучения информатике с педагогическими, психологическими и гуманитарными дисциплинами, в том числе на основе интеграции деятельности в области информатики и	знать: - методы организации учебной деятельности при изучении понятий информационной безопасности курса информатики; - этапы формирования понятий информационной безопасности в обучении информатике; уметь: - организовывать учебную деятельность для овладения способами защиты информации, изучаемые в школьном

методики обучения информатики.	курсе информатики; - проектировать политику информационной безопасности в условиях определенной образовательной организации; владеть: - методами, средствами и формами организации информационной безопасности в соответствии с принятыми - правовыми нормами РФ; - подходами к формированию умений использовать современные методы защиты информации.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Девятый семестр	Десятый семестр
Контактная работа (всего)	**80**	**32**	**48**
Лекции	24		24
Практические	56	32	24
Самостоятельная работа (всего)	**64**	**40**	**24**
Виды промежуточной аттестации			
Зачет		+	+
Общая трудоемкость часы	**144**	**72**	**72**
Общая трудоемкость зачетные единицы	**4**	**2**	**2**

5. Содержание дисциплины

5.1. Содержание разделов дисциплины

Раздел 1. Нормативно-правовые средства защиты информации в образовательной организации:

Информационные ресурсы по информационной безопасности в сфере образования. Правовые вопросы, связанные с информационной безопасностью в образовании. Нормативные документы, касающиеся конфиденциальной информации в образовательной организации.

Раздел 2. Программные средства защиты информации в образовательной организации:

Программные и аппаратные средства, связанные с угрозой обеспечения информационной безопасности к конфиденциальной информацией в образовательных организациях. Брандмауэр как аппаратное и программное средство ограничения доступа к информации. Комплексная защита сетевого компьютера от информационных угроз в образовательной организации. DoS- и DDoS-атаки как инструмент ограничения доступа к сетевому образовательному ресурсу. Вопросы организации информационной безопасности при работе с информационными образовательными ресурсами и сервисами сети Интернет.

Раздел 3. Практические вопросы организации информационной безопасности в образовательной организации:

Антивирусные программные средства образовательной организации. Парольная защита. Социальная инженерия и ее методы.

Раздел 4. Организация защиты информации в образовательных организациях:

Программы шифрования данных. Социальные сети как информационная угроза для школьников. Социальные сети в образовательной среде. Школьники и сеть Интернет. Политика информационной безопасности и ее организация в локальной сети образовательной организации.

5.2. Содержание дисциплины: Лабораторные (40 ч.)

10 семестр. Лекции (24 ч.)

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

Тема 1. Информационная безопасность как наука и деятельность (2 ч.)

Понятие и принципы информационной безопасности. Общие термины и определения. Информационная безопасность в образовательной организации.

Тема 2. Виды возможных нарушений информационной безопасности в образовательной организации(2 ч.)

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

Тема 3. Причины возникновения информационных угроз и меры защиты от них (2 ч.)

Информационная угроза. Виды информационных угроз в образовательной организации. Способы защиты от информационных угроз.

Тема 4. Вредоносное программное обеспечение и меры защиты от него (2 ч.)

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

Тема 5. Понятие о видах вирусов. Антивирусная защита компьютера образовательной организации (2 ч.)

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

Тема 6. Технология построения защищенных информационных систем образовательной организации (2 ч.)

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

Раздел 4. Организация защиты информации в образовательных организациях (12 ч.)

Тема 7. Криптография как наука (2 ч.)

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

Тема 8. Психологическое воздействие на участника образовательного процесса как информационная угроза. (2 ч.)

Способы психологического воздействия. Способы защиты от воздействия.

Тема 9. Безопасность персональных данных участников образовательного процесса. (2 ч.)

Персональные данные. Причины несанкционированного доступа к персональным

данным в образовательной организации. Способы противодействия незаконного доступа к персональным данным. Законодательство в области персональных данных.

Тема 10. Результаты интеллектуальной деятельности и правовое обеспечение безопасности их использования. (2 ч.)

Интеллектуальные права. Распоряжение интеллектуальными правами. Правовая защита интеллектуальных прав в области образовательной литературы.

Тема 11. 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. Электронная подпись организаторов ЕГЭ и ОГЭ.

Тема 12. 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. Защита информации в образовательной организации.

9 семестр. Практические (32 ч.)

Раздел 1 Нормативно-правовые средства защиты информации в образовательной организации (16 ч.)

Тема 1. Общие вопросы информационной безопасности в сфере образования (2 ч.)

Теоретические вопросы организации информационной безопасности. Пути организации информационной безопасности в образовательной организации. Информационные ресурсы по информационной безопасности.

Тема 2. Информационные ресурсы по информационной безопасности в сфере образования (2 ч.)

Информационная безопасность в периодике и ресурсах сети Интернет. Сайты, посвященные информационной безопасности. Основы информационной безопасности в образовательной среде.

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

Правовое регулирование в области информационной безопасности. Законы о преступлениях в сфере информационных технологий.

Тема 4. Правовые вопросы, связанные с информационной безопасностью в образовании (2 ч.)

Авторское право. Пути доказательства авторства. Законодательная база по информационной безопасности в образовательных организациях

Тема 5. Интеллектуальная собственность и меры по ее соблюдению в образовательной организации (2 ч.)

Интеллектуальная собственность. Способы защиты интеллектуальной собственности. Лицензионное программное обеспечение. Лицензии в образовательной среде.

Тема 6. Компьютерное пиратство и законодательная ответственность за него (2 ч.)

Компьютерные пираты. Способы совершения компьютерного пиратства. Законодательство РФ в области компьютерного пиратства.

Тема 7. Нормативные документы, касающиеся конфиденциальной информации в образовательной организации (2 ч.)

Государственная тайна. Ответственность за разглашение государственной тайны.

Состояние законодательства РФ в области сохранения государственной тайны. Примеры нарушения государственной тайны

Тема 8. Нормативные документы, касающиеся государственной тайны (2 ч.)

Решения ситуационных задач на нарушение государственной тайны.

Раздел 2. Программные средства защиты информации в образовательной организации (16 ч.)

Тема 9. Программные и аппаратные средства, связанные с угрозой обеспечения информационной безопасности к конфиденциальной информации в образовательных организациях (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 10. Программные и аппаратные средства, связанные с угрозой обеспечения информационной безопасности (2 ч.)

USB-накопители на информационная угроза. Ограничение доступа к USB-накопителям в образовательных организациях.

Разграничение доступа в локальных сетях. Взлом учетных записей пользователей локальной сети. Способы предотвращения взлома.

Тема 11. DoS- и DDoS-атаки как инструмент ограничения доступа к сетевому образовательному ресурсу (2ч.)

Технология проведения DoS- и DDoS-атак. Анализ подобных атак на сайты образовательных организаций и образовательные ресурсы.

Тема 12. Комплексная защита сетевого компьютера от информационных угроз в образовательной организации (2 ч.)

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

Тема 13. Хакерство как угроза информационной безопасности образовательной организации (2 ч.)

Хакинг и антихакинг. Хакерские технологии. Противостояние хакерству.

Тема 14. 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 15. Вопросы организации информационной безопасности при работе с информационными образовательными ресурсами и сервисами сети Интернет (2 ч.)

Образовательный информационный ресурс (контент). Правила безопасной работы с контентом. Фильтрация.

Тема 16. Итоговое тестирование (2 ч.)

Итоговое тестирование на проверку сформированности знаний и умений в области теоретико-практических основ информационной безопасности.

10 семестр. Практические (24 ч.)

Раздел 3. Практические вопросы организации информационной безопасности в образовательной организации (12 ч.)

Тема 17. Антивирусные программные средства образовательной организации (2 ч.)

Вредоносное программное обеспечение и пути его попадания в компьютеры образовательных организаций. Клавиатурные шпионы (кейлоггеры) и необходимость их использования в образовательной организации. Функциональные возможности антивирусных программных средств.

Тема 19. Онлайн инструменты для антивирусной защиты информации сетевых компьютеров образовательной организации (2 ч.)

Онлайн-антивирусы. Обзор онлайн-антивирусов. Способы работы.

Sms-блокеры и методы борьбы с ними.

Тема 20. Парольная защита (2 ч.)

Пароль как средство ограничения доступа к ресурсу. Требования к выбору пароля. Хранители паролей. Целесообразность использования хранителей паролей в образовательной организации. Программы восстановления (взлома) паролей. Брутфорс.

Тема 21. Программы шифрования данных (2 ч.)

Шифрование данных и его назначение. Алгоритмы и стандарты шифрования. Необходимость шифрования данных в образовательных организациях. Архивирование файлов с паролем как инструмент защиты от несанкционированного доступа

Тема 22. Политика информационной безопасности и ее организация в локальной сети (2ч.)

Технология организации локальных компьютерных сетей в образовательной организации. Правила работы в таких сетях. Разграничение доступа.

Раздел 4. Организация защиты информации в образовательных организациях (12 ч.)

Тема 23. Криптография и ее методы шифрования информации.

Криптография как научная область.

Генезис криптографии. Методы криптографической защиты информации.

Программы средства для шифрования данных.

Тема 24. Социальная инженерия и ее методы (2 ч.)

Обзор методов социальной инженерии. Социальная инженерия как угроза образовательной организации. 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 25. Социальная инженерия и ее методы (2 ч.)

Социальные сети как инструмент образования. Решение проблемы дезинформации через социальные сети.

Тема 26. Социальная инженерия и ее методы (2 ч.)

Фарминг как инструмент скрытого перенаправления на поддельные сайты. Фишинг и вишинг как инструмент получения конфиденциальной информации. Интернет-мошенничество к представителям образовательных организаций. Правила поведения участников образовательного процесса в сети Интернет при работе с информационными ресурсами.

Тема 27. Школьники и сеть Интернет (2 ч.)

Информационные ресурсы для школьников. Способы обучения школьников работе с

информационными ресурсами сети Интернет. Разъяснительные мероприятия о пользе и вреде информационного контента сети Интернет.

Тема 28. Социальные сети как информационная угроза (2 ч.)

Социальные сети: назначение, способы работы с информацией, информационный контент. Технология информационных атак на школьников через социальные сети. Меры противодействия со стороны учителей и родителей.

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

6.1 Вопросы и задания для самостоятельной работы

Девятый семестр (40 ч.)

Раздел 1. Проблемы информационной безопасности в современном обществе (20 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 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: 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 (20 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

Bit Defender

Total Security Norton и др.

Программы проактивной защиты и защиты от шпионских программ

WinPatrol

Ad-Aware

SUPER

AntiSpyware

Spyware Doctor

AVZ и др.

Десятый семестр (24 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 (12 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-11.2 Проектирует и решает исследовательские задачи в предметной области в			

соответствии с профилем и уровнем обучения и в области образования.			
Не способен проектировать и решать исследовательские задачи в предметной области в соответствии с профилем и уровнем обучения и в области образования.	В целом успешно, но бессистемно проектирует и решает исследовательские задачи в предметной области в соответствии с профилем и уровнем обучения и в области образования.	В целом успешно, но с отдельными недочетами проектирует и решает исследовательские задачи в предметной области в соответствии с профилем и уровнем обучения и в области образования.	Способен в полном объеме проектировать и решать исследовательские задачи в предметной области в соответствии с профилем и уровнем обучения и в области образования.
ПК-14 Способен устанавливать содержательные, методологические и мировоззренческие связи предметной области (в соответствии с профилем и уровнем обучения) со смежныминаучными областями			
ПК-14.3 Формирует междисциплинарные связи информатики с предметами естественнонаучного цикла.			
Не способен формировать междисциплинарные связи информатики с предметами естественнонаучного цикла.	В целом успешно, но бессистемно формирует междисциплинарные связи информатики с предметами естественнонаучного цикла.	В целом успешно, но с отдельными недочетами формирует междисциплинарные связи информатики с предметами естественнонаучного цикла.	Способен в полном объеме формировать междисциплинарные связи информатики с предметами естественнонаучного цикла.

Уровень сформированности	Шкала оценивания для промежуточной аттестации		Шкала оценивания по БРС
компетенции	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

Девятый семестр (Зачет, ПК-11.1, ПК-11.2, ПК -14.3)

1. Перечислите и обоснуйте основные задачи системы информационной безопасности.
2. Укажите и обоснуйте этапы развития информационной безопасности.

3. Сформулируйте определение защиты информации, укажите основные аспекты защиты информации и обоснуйте их целесообразность.

4. Охарактеризуйте программные средства, необходимые для организации информационной безопасности при работе на компьютере. На примере одного программного средства раскройте его функциональные возможности по защите информации.

5. Охарактеризуйте программные средства, необходимые для организации информационной безопасности в компьютерной сети. На примере одного программного средства раскройте его функциональные возможности по защите информации.

6. Охарактеризуйте аппаратные средства, необходимые для организации информационной безопасности. Приведите примеры аппаратных средств защиты информации.

7. Охарактеризуйте аппаратные средства, необходимые для организации информационной безопасности в компьютерной сети. 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.

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

12. Дайте определение государственной тайны. Перечислите основные статьи в Федеральном 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 в России. Охарактеризуйте нарушения, представленные в этих документах и меру наказания.

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

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

18. Охарактеризуйте аппаратные средства защиты информации, и их классификации. Приведите примеры аппаратных средств защиты информации в образовательной организации.

19. Охарактеризуйте программные средства защиты информации, и их классификации. Перечислите основные средства программной защиты информации. На примере одного приложения раскройте его функциональные возможности по защите информации.

20. Опишите способы организации информационной безопасности несовершеннолетних пользователей.

21. Проанализируйте важность и значимость организации информационной безопасности в образовательных организациях.

22. Расскажите о новых тенденциях в развитии информационной безопасности в образовательных учреждениях.

23. Опишите стратегию организации информационной безопасности в образовательном учреждении.

24. Проведите обзор современных средств защиты информации.

25. Раскройте различные подходы к определению понятия «информационная безопасность». Приведите примеры нарушения информационной безопасности в быту и в образовательной организации.

Десятый семестр (Зачет, ПК-11.1, ПК-11.2, ПК -14.3)

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

2. Раскройте суть нормативно-правового аспекта защиты информации в образовательной организации.

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

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

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

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

7. Дайте понятие политики информационной безопасности. Опишите способы организации политики информационной безопасности в образовательной организации

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

9. Охарактеризуйте организационные меры защиты информации в образовательной организации. Обоснуйте основные мероприятия по обеспечению информационной безопасности.

10. Охарактеризуйте технологические меры информационной безопасности в образовательной организации. 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 образовательной организации.

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 участников образовательного процесса.

27. Раскройте суть социальной инженерии. Опишите ее методы.

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

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

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

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

32. Раскройте суть электронной цифровой подписи. Охарактеризуйте правовой и технический аспекты. Сформулируйте рекомендации для использования электронной цифровой подписи в образовательной сфере.

33. 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.

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

Итоговая оценка выставляется с учетом набранной суммы баллов.

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. 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. 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. – Текст : электронный.

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. – Текст : электронный.

Дополнительная литература

1. Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Южный федеральный университет. – Ростов-на-Дону : Южный федеральный университет, 2016. – 74 с. : схем., табл., ил. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=493175. – Текст : электронный.

2. Сагдеев, К. М. Физические основы защиты информации [Электронный ресурс] : учебное пособие / 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.informika.ru - Федеральное государственное автономное учреждение «Государственный научно-исследовательский институт информационных технологий и телекоммуникаций» [Электронный ресурс] / М.: Informika.ru, 2002 - 2016. – Режим доступ : http://www.informika.ru

3. http://www.securrity.ru – SecuRRity.Ru – «Информационная безопасность компьютерных систем и защита конфиденциальных данных»

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 готовностьк 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 информационно-справочных систем

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

12.2 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, экспорт информации 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.