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

Физико-математический факультет

Кафедра информатики и вычислительной техники

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Наименование дисциплины (модуля): Информационная безопасность в образовании

Уровень ОПОП: Бакалавриат

Направление подготовки: 44.03.05 Педагогическое образование (с двумя профилями подготовки)

Профиль подготовки: Информатика. Математика

Форма обучения: Очная

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

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 № 12 от 20.06.2019 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 - изучение основ информационной безопасности, формирование у студентов информационного мировоззрения на основе знания аспектов защиты информации с использованием естественнонаучных и математических знаний для реализации образовательных программ по информатике; воспитание информационной культуры для эффективного применения полученных знаний в профессиональной деятельности и достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса.

Задачи дисциплины:

- изучение основных направлений организации информационной безопасности (правового, технического, аппаратного) для реализации образовательных программ по информатике;
- изучение основ правового регулирования информационной безопасности в России для реализации образовательных программ по информатике;
- формирование представлений о технических способах и средствах обеспечения защиты информации с использованием естественнонаучных и математических знаний для ориентирования в современном образовательном пространстве;
- изучение программных средств обеспечения информационной безопасности при работе на ПК и в сети Интернет с использованием возможностей образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса;
- формирование умений аргументированного выбора и самостоятельной установки соответствующего программного обеспечения по защите данных на ПК для реализации образовательных программ по информатике;
- формирование умений по организации защиты файлов и отдельных данных в документах Microsoft для реализации образовательных программ по информатике;
- формирование умений разрабатывать и реализовывать политику информационной безопасности на предприятии, в частности в образовательном учреждении.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина Б1.В.ДВ.05.02 «Информационная безопасность в образовании» относится к вариативной части учебного плана.

Дисциплина изучается на 3 курсе, в 5, 6 семестрах.

Для изучения дисциплины требуется: знание возможностей сервисов сети Интернет

знать:

– определение понятия информации;
– свойства информации;
– Информационные процессы;
– носители информации;
– архитектуру ПК;
– классификацию программного обеспечения;
– структуру операционной системы Windows;
– понятие правового пространства, уровни законодательства в России;

основы дистанционных образовательных технологий;

уметь:

– применять свободное программное обеспечение, служащее ля выполнения вспомогательных операций обработки данных или обслуживания компьютеров;
– применять дистанционные технологии в образовании; владеть:
– программными продуктами Microsoft.

владеть понятием информация, знать свойства информации, распознавать информационные процессы и носители информации;

– знать архитектуру ПК, классификацию программного обеспечения, структуру операционной системы Windows;

–владеть

– программными продуктами Microsoft;

Изучению дисциплины «Информационная безопасность в образовании» предшествует освоение дисциплин (практик):

Информационные технологии в образовании.

Освоение дисциплины «Информационная безопасность в образовании» является необходимой основой для последующего изучения дисциплин (практик):

Компьютерные сети; Интернет технологии;

История и методология информатики и вычислительной техники.

Область профессиональной деятельности, на которую ориентирует дисциплина

«Информационная безопасность в образовании», включает: 01 Образование и наука (в сфере дошкольного, начального общего, основного общего, среднего общего образования, профессионального обучения, профессионального образования, дополнительного образования).

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 общекультурными компетенциями (ОК):

ОК-3. способность использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве

ОК-3. способность использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве	знать: - фундаментальные понятия информационной безопасности для формирования способности для формирования способности использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве; - естественнонаучные и математические факты, в том числе основные аспекты информационной безопасности для ориентирования в современном информационном пространстве; уметь: - определять оптимальный набор программных средств для обеспечения безопасной работы на компьютере для безопасного ориентирования в современном информационном пространстве; владеть: - методами организации комплексной защиты информации (компьютерной, конфиденциальной) для ориентирования в современном информационном пространстве с помощью естественнонаучных и математических знаний.

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 информационной безопасности, изучаемые в школьном курсе информатики с целью реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов; уметь: - использовать способы защиты информации, изучаемые в школьном курсе информатики в условиях реализации

	образовательных программ по информатике в соответствии с требованиями образовательных стандартов;; владеть: - современными методами защиты информации с целью реализации образовательных программ по информатике в соответствии с требованиями образовательных стандартов.
ПК-4. способностью использовать возможности образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса средствами преподаваемых учебных предметов **педагогическая деятельность**	
ПК-4 способностью использовать возможности образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса средствами преподаваемых учебных предметов	знать: - нормативные документы, отражающие концепцию информационной безопасности в РФ для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса средствами преподаваемых учебных предметов; уметь: - проектировать политику информационной безопасности в условиях определенной образовательной организации с использованием возможностей информационно-образовательной среды; владеть: - методами, средствами и формами организации информационной безопасности в соответствии с принятыми правовыми нормами РФ для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Пятый семестр	Шестой семестр
Контактная работа (всего)	**54**	**18**	**36**
Практические	36	18	18
Лекции	18		18
Самостоятельная работа (всего)	**38**	**18**	**20**
Виды промежуточной аттестации	**52**		**52**
Зачет		+	
Экзамен	52		52
Общая трудоемкость часы	**144**	**36**	**108**
Общая трудоемкость зачетные единицы	**4**	**1**	**3**

5. Содержание дисциплины

5.1. Содержание модулей дисциплины

Модуль 1. Нормативно-правовые средства защиты информации:

Основные понятия информационной безопасности. Правовой аспект защиты информации. Организационный аспект информационной безопасности. Понятие информационной угрозы, виды угроз. Методы и средства защиты информации.

Модуль 2. Программные средства защиты информации:

Классификатор российского ПО, программное обеспечение для реализации информационной безопасности. Браузеры. Антивирусные программы. Программные средства защиты информации на ПК. Защита информации в компьютерных сетях.

Модуль 3. Практические вопросы организации информационной безопасности:

Криптографические методы защиты инофрмации. Исторические шифры. Математические основы современных шифров.Позиционные системы счисления. Гаммирование.

Модуль 4. Организация защиты информации в образовательных организациях:

Политика информационной безопасности в образовательной организации. Нормативные

документы о защите детей в информационном простанстве. Формирование информационной культуры у детей при использовании сети интернет. Информационная безопасность на уроках инофрматики.

1.1. Содержание дисциплины: Лекции (18 ч.)

Модуль 3. Практические вопросы организации информационной безопасности (8 ч.)

Тема 1. Назначение и задачи обеспечения информационной безопасности в сфере образования (2 ч.)

Информационная безопасность как научная область.

Направления обеспечения информационной безопасности в современных условиях. Необходимость соблюдения информационной безопасности в образовательных организациях.

Тема 2. Причины возникновения в образовательных организациях информационных угроз и меры защиты от них (2 ч.)

Информационная угроза. Виды информационных угроз применительно к сфере образования. Способы защиты и предотвращения от информационных угроз.

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

Нарушение информационной безопасности. Уровни нарушения информационной безопасности в образовательной организации: аппаратный, программный, человеческий фактор. Меры профилактики нарушений.

Тема 4. Теория информационной безопасности и ее основные направления (2 ч.) Теоретические вопросы организации информационной безопасности в образовательной организации. Методические разработки по обеспечению безопасной работы с информацией в компьютерной сети образовательной организации.

Модуль 4. Организация защиты информации в образовательных организациях (10 ч.)

Тема 5. Общие вопросы организации информационной безопасности в образовании (2

Государственная защита информации.

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

Тема 6. Понятие о видах вирусов. Антивирусная защита компьютеров в образовательных организациях (2 ч.)

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

Классификация компьютерных вирусов.

Способы защиты от компьютерных вирусах в образовательных организациях.вирусов

Тема 7. 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 8. 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 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.

Необходимость использовать данные виды программ в образовательной организации.

5.2. Содержание дисциплины: Практические (36 ч.)

Модуль 1. Правовые вопросы защиты информации в компьютерных сетях (8 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.

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

Тема 5. Программные и аппаратные средства, связанные с угрозой обеспечения информационной безопасности (2 ч.)

Несанкционированный доступ к аппаратным средствам компьютера и средства ограничения доступа.

Взлом экранной заставки Windows и пароля BIOS. Способы предотвращения взлома. Взлом операционной системы посредством носителей информации. Способы защиты. 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 ресурс (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 защит 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 ата 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 3. Практические вопросы организации информационной безопасности (8 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.

Модуль 4. Организация защиты информации в образовательных организациях (10 *ч.)*

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

Пятый семестр (9 ч.)

Модуль 1. Нормативно-правовые средства защиты информации

Вид СРС: *Выполнение индивидуальных заданий

Подготовка ситуационных задач по информационной безопасности на основании статей соответствующих законов и нормативных актов РФ. Возможные разделы:

Раздел «АВТОРСКОЕПРАВО» 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 з 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» 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» друг 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. Программные средства защиты информации.

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!

Шестой семестр (10 ч.)

Модуль 3. Практические вопросы организации информационной безопасности

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 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 Avira Free Antivirus FreeFixer

Comodo AntiVirus

Microsoft Malicious Software Removal Tool DefenseWall HIPS

Trend Micro RootkitBuster ClamWin

ClamAV

Malwarebytes Anti-Malware NANO Антивирус

Anti Trojan Elite PC Tools AntiVirus Online Armor VirusBuster TrojanHunter Prevx CSI REMSES

The Cleaner

Программы для восстановления данных FineRecovery

FBackup DiskDigger

MiniTool Power Data Recovery CardRecovery

Recuva UndeleteMyFiles FileRescue Pro R-Studio

Recover My Files Active@ UNDELETE

Защита детей от интернет угроз CTracker Pro

PC TimeWatch Power Spy Kidlogger iProtectYou Pro

МОЖНО ВЫБРАТЬ СВОИ ПРОГРАММНЫЕ СРЕДСТВА, НЕ УКАЗАННЫЕ ВЫШЕ!

Модуль 4. Организация защиты информации в образовательных организациях

Вид СРС: *Подготовка к промежуточной аттестации

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

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
ОК-3 ПК-1	3 курс, Пятый семестр	Зачет	Модуль 1: Нормативно-правовые средства защиты информации
ПК-4	3 курс, Пятый семестр	Зачет	Модуль 2: Программные средства защиты информации.
ОК-3 ПК-1	3 курс, Шестой семестр	Экзамен	Модуль 3: Практические вопросы организации информационной безопасности
ПК-4	3 курс, Шестой семестр	Экзамен	Модуль 4: Организация защиты информации в образовательных организациях

Сведения об иных дисциплинах, участвующих в формировании данных компетенций:
Компетенция ОК-3 формируется в процессе изучения дисциплин:

Вводный курс математики, Геометрия, Естественнонаучная картина мира, Защита информации в компьютерных сетях, Информационная безопасность в образовании, Информационные технологии в образовании, История математики, Основы математической обработки информации.

Компетенция ПК-1 формируется в процессе изучения дисциплин:

3D моделирование, Алгебра, Вводный курс математики, Внеурочная деятельность учащихся по информатике, Геометрия, Задачи с параметрами и методы их решения, Защита информации в компьютерных сетях, Интернет-технологии, Информационная безопасность в образовании, Информационные системы, Искусственный интеллект и экспертные системы, Исследовательская и проектная деятельность в обучении математике, Исследовательская и проектная деятельность учащихся по информатике, Исторический подход в обучении математике, Компетентностный подход в обучении математике, Компьютерная алгебра,

Компьютерная графика, Компьютерное моделирование, Компьютерные сети, Математический анализ, Математическое моделирование, Методика обучения информатике, Методика обучения математике, Методика обучения математике в профильных классах, Методология обучения математике, Методы аксиоматического построения алгебраических систем, Методы решения задач ГИА по математике, Методы решения задач по информатике, Моделирование в системах динамической математики, Нестандартные методы решения математических задач, Общая теория линейных операторов и ее приложение к решению геометрических задач, Оптимизация и продвижение сайтов, , Практикум по информационным технологиям, , Применение систем динамической математики в образовании,

Программирование, Проектирование в системах автоматизированного проектирования, Проектирование информационно-образовательной среды, Разработка приложений в Microsoft Visual Studio, Разработка электронны образовательных ресурсов и методика их оценки, Реализация прикладной направленности в обучении математике, Решение задач повышенного уровня сложности по алгебре, Решение задач повышенного уровня сложности по геометрии, Решение олимпиадных задач по информатике, Свободное программное обеспечение в образовании, Свободные инструментальные системы, Системы компьютерной математики, Современные средства оценивания результатов обучения, Теоретические основы информатики, Теория рядов и ее приложения, Технология обучения математическим понятиям в школе, Технология обучения учащихся решению математических задач, Технология разработки и методика проведения элективных курсов по математике, Физика, Формы и методы работы с одаренными детьми по математике, Численные методы, Элементарная математика, Элементы конструктивной геометрии в школьном курсе математики, Элементы функционального анализа.

Компетенция ПК-4 формируется в процессе изучения дисциплин:

3D моделирование, Защита информации в компьютерных сетях, Интернет-технологии, Информационная безопасность в образовании, Информационные системы, Исследовательская и проектная деятельность в обучении математике, Компьютерная графика, Компьютерное моделирование, Компьютерные сети, Математическое моделирование, Методика обучения информатике, Методика обученияматематике, Методика обучения математике в профильных классах, Методика подготовки учащихся к ГИА по информатике, Методы решения задач ГИА по математике, Методы решения задач по информатике, Моделирование в системах динамической математики, Нестандартные методы решений математических задач, Оптимизация и продвижение сайтов, Педагогическая практика, 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, Практикум по информационным технологиям, Преддипломная практика, Применение систем динамической математики в образовании, Программирование, Проектирование в системах автоматизированного проектирования, Проектирование информационно-образовательной среды, Разработка приложений в Microsoft Visual Studio Разработка электронных образовательных ресурсов и методика их оценки, Решение задач повышенного уровня сложности по алгебре, Решение задач повышенного уровня сложности по геометрии, Решение олимпиадных задач по информатике, Свободное программное обеспечение в образовании, Свободные инструментальные системы, Системы компьютерной математики, Теоретические основы информатики, Технология разработки и методика проведения элективных курсов по информатике, Технология разработки и методика проведения элективных курсов по математике, Физика, Формы и методы работы с одаренными детьми по математике, Численные методы.

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	Студент знает: фундаментальные понятия информационной безопасности; аспекты информационной безопасности; основные подходы к разработке политики информационной безопасности; нормативно-правовые документы на всех государственных уровнях, ре-гламентирующих организацию защиты информации в РФ; функционал аппаратно-программного обеспечения и сервисы Интернет с целью организации защиты компьютерной информации в процессе профессиональной деятельности; правила предостережения от интернет-мошенничества; основные способы защиты компьютерной информации; способы шифрования данных Владеет средствами обеспечения информационной безопасности при работе за персональным компьютером и в компьютерных сетях; криптографическими методами защиты информации; методами организации комплексной защиты информации (компьютерной, конфиденциальной)
Незачтено	Студент демонстрирует незнание основных понятий содержания дисциплины, обнаруживая существенные пробелы в знаниях учебного материала, допускает принципиальные ошибки в выполнении практических заданий; затрудняется делать выводы и отвечать на дополнительные вопросы преподавателя.
Отлично	Студент знает: основные понятия информационной безопасности; нормативно-правовую базу, аспекты организации ИБ, современные методы и средства ИБ, основы криптографии, современные криптосистемы; демонстрирует умение применять способы защиты информации на ПК и в компьютерных сетях; владеет методами криптографической защиты информации. Ответ логичен и последователен, отличается глубиной и полнотой раскрытия темы, выводы доказательны.

Хорошо	Студент демонстрирует знание и понимание основного содержания дисциплины. Экзаменуемый знает основные основные понятия информационной безопасности, нормативно-правовую базу, аспекты организации ИБ, современные методы и средства ИБ, основы криптографии, современные криптосистемы; демонстрирует умение применять способы защиты информации на ПК и в компьютерных сетях; умеет применять криптографические методы защиты информации; владеет терминологией, однако в ответе допускаются одна-две неточности. Студент дает логически выстроенный, достаточно полный ответ по вопросу.
Удовлетворительно	Студент имеет представления об основных понятиях информационной безопасности; демонстрирует некоторые умения применять способы защиты информации на ПК и в компьютерных сетях; формулирует аргументированные ответы на дополнительные вопросы преподавателя и приводить примеры; однако слабо владеет методами криптографии. Допускается несколько ошибок в содержании ответа, при этом ответ отличается недостаточной глубиной и полнотой раскрытия темы.
Неудовлетворительно	Студент демонстрирует незнание основного содержания дисциплины, обнаруживая существенные пробелы в знаниях учебного материала, допускает принципиальные ошибки в выполнении предлагаемых заданий; затрудняется делать выводы и отвечать на дополнительные вопросы преподавателя.

8.3. Вопросы, задания текущего контроля

Модуль 1: Правовые вопросы защиты информации в компьютерных сетях

ОК-3 способность использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве

1. Описать процедуру установки на компьютер антивирусного программного средства (из списка)

2. Раскройте понятие «информационная безопасность». Приведите примеры нарушения информационной безопасности на предприятии.

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

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

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

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

1. Сделать анализ нормативной базы по реализации информационной безопасности в образовательных учреждениях.

2. Описать процедуру разработки политики информационной безопасности для школы.

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

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

5. Расскажите о применении математики и других областей знаний в информационной безопасности.

Модуль 2: Программные средства и сервисы сети Интернет по защите информации

ПК-4 способность использовать возможности образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса средствами преподаваемых учебных предметов

1. Раскройте основные аспекты ИБ, изучаемые на уроках информатики (укажите основные разделы курса школьной информатики).

2. Сформулируйте впоросы ИБ, целесообразные для организации внеурочной деятельности (внеклассные мероприятия).

3. Разработайте кейс-задачи для школьников для разработки политики ИБ.

4. Разработайте кейс-задачи для школьников, направленные на формирование информационной культуры (поведение в социальных сетях).

5. Разработайте кейс-задачи для школьников, направленные на формирование информационной культуры (платежные системы).

6. Разработайте кейс-задачи для школьников, направленные на формирование информационной культуры (дистанционные государственные услуги).

Модуль 3. Практические вопросы организации информационной безопасности

ОК-3 способностью использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве

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

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

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

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

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

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

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

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

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

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

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

Модуль 4. Организация защиты информации в образовательных организациях

ПК-4 способностью использовать возможности образовательной среды для достижения личностных, метапредметных и предметных результатов обучения и обеспечения качества учебно-воспитательного процесса средствами преподаваемых учебных предметов

Вопросы и задания для устного опроса:

1. Раскройте основные аспекты ИБ, изучаемые на уроках информатики (укажите основные разделы курса школьной информатики).

2. Сформулируйте впоросы ИБ, целесообразные для организации внеурочной деятельности (внеклассные мероприятия).

3. Разработайте кейс-задачи для школьников для разработки политики ИБ.

4. Разработате кейс-задачи для школьников,направленные на формирование информационной культуры (поведение в социальных сетях).

5. Разработате кейс-задачи для школьников, направленные на формирование информационной культуры (платежные системы).

6. Разработайте кейс-задачи для школьников, направленные на формирование

информационной культуры (дистанционные государственные услуги).

8.4. Вопросы промежуточной аттестации

Пятый семестр (Зачет, ОК-3, ПК-1,ПК-4)

1. Раскройте различные подходы к определению понятия «информационная безопасность». Приведите примеры нарушения информационной безопасности в быту и в образовательном учреждении.
2. Перечислите и обоснуйте основные задачи системы информационной безопасности.
3. Укажите и обоснуйте этапы развития информационной безопасности.
4. Сформулируйте определение защиты информации, укажите основные аспекты защиты информации и обоснуйте их целесообразность.
5. Охарактеризуйте программные средства, необходимые для организации информационной безопасности при работе на компьютере. На примере одного программного средства раскройте его функциональные возможности по защите информации.
6. Охарактеризуйте программные средства, необходимые для организации информационной безопасности в компьютерной сети. На примере одного программного средства раскройте его функциональные возможности по защите информации.
7. Охарактеризуйте аппаратные средства, необходимые для организации информационной безопасности. Приведите примеры аппаратных средств защиты информации.
8. Охарактеризуйте аппаратные средства, необходимые для организации информационной безопасности в компьютерной сети. Приведите примеры аппаратных средств защиты информации.
9. Укажите основные направления организации информационной безопасности. Сформулируйте рекомендации для организации информационной безопасности при работе на ПК для сотрудников образовательного учреждения.
10. Раскройте понятие «сетевые атаки». Приведите примеры сетевых атак. Укажите способы несанкционированного проникновения на сетевой компьютер и охарактеризуйте пути противодействия им.
11. Раскройте понятие «информационная угроза» с позиции проблемы обеспечения информационной безопасности. Охарактеризуйте виды угроз, приведите примеры.
12. Раскройте суть нормативно-правового аспекта защиты информации. Охарактеризуйте структуру законодательства России в области защиты информации.
13. Дайте определение государственной тайны. Перечислите основные статьи в Федеральном Законе о государственной тайне.
14. Дайте определение понятиям «авторское право» и «коммерческая тайна». Укажите их отличительные особенности. Охарактеризуйте способы защиты авторских прав и коммерческой тайны.
15. Перечислите виды конфиденциальной информации. Приведите примеры конфиденциальной информации и укажите способы ее защиты.
16. Перечислите нормативно-правовые документы, ориентированные на обеспечение информационной безопасности в России. Охарактеризуйте нарушения, представленные в этих документах и меру наказания.
17. Охарактеризуйте аппаратные средства защиты информации, и их классификации. Приведите примеры аппаратных средств защиты информации в образовательной организации.
18. 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.
19. Перечислите антивирусные программные средства. На примере конкретного приложения продемонстрируйте настройку безопасности.
20. Раскройте понятие «компьютерный вирус». Перечислите виды компьютерных вирусов. Приведите примеры, опишите способы их проникновения и особенности разрушительных действий.
21. Перечислите способы проникновения компьютерных вирусов на ПК и опишите механизм их реализации. Приведите примеры, опишите особенности их разрушительных действий.

22. Раскройте технологию антивирусной защиты сетевого компьютера. Приведите примеры антивирусных приложений и укажите особенности их функционала.

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

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

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

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

Шестой семестр (Экзамен, ОК-3, ПК-1, ПК-4)

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

2. Охарактеризуйте структуру законодательства РФ в области защиты информации в образовательных организациях.

3. Перечислите нормативно-правовые документы, ориентированные на обеспечение информационной безопасности в России. Охарактеризуйте материалы, представленные в этих документах.

4. Дайте определение государственной тайны. Перечислите основные статьи в Федеральном Законе о государственной тайне. Затрагивают ли данные статьи сферу образования?

5. Дайте определение понятиям «авторское право» и «коммерческая тайна». Укажите их отличительные особенности. Охарактеризуйте способы защиты авторских прав и коммерческой тайны применительно к образовательным организациям.

6. Перечислите виды конфиденциальной информации. Приведите примеры конфиденциальной информации, которая может относиться к образовательным организациям, и укажите способы ее защиты.

7. Перечислите нормативно-правовые акты, регламентирующие обращение с персональными данными. Приведите примеры внутренних нормативных актов в образовательных организациях о персональных данных.

8. Раскройте понятие «информационная безопасность». Приведите примеры нарушения информационной безопасности в образовательных организациях.

9. Дайте понятие политики информационной безопасности. Опишите способы организации политики информационной безопасности в образовательных организациях.

10. Расскажите о программных средствах, используемых для обеспечения информационной безопасности при работе на компьютере в образовательных организациях.

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

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

13. Раскройте основные направления организации информационной безопасности. Сформулируйте рекомендации для обеспечения информационной безопасности при работе на компьютере для педагогов.

14. Раскройте основные направления обеспечения информационной безопасности в компьютерной сети в образовательной организации. Сформулируйте рекомендации для обеспечения информационной безопасности при работе на сетевом компьютере для педагога.

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

16. Раскройте понятие «информационная угроза» с позиции проблемы обеспечения

информационной безопасности в образовательной организации. Охарактеризуйте виды угроз, приведите примеры.

17. Раскройте суть нормативно-правового аспекта защиты информации в образовательных организациях.

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

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

20. Охарактеризуйте организационные меры защиты информации в образовательных организациях. Обоснуйте основные мероприятия по обеспечению информационной безопасности.

21. Охарактеризуйте технологические меры информационной безопасности в образовательных организациях. Обоснуйте классификацию средств технологической защиты информации.

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

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

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

25. Раскройте технологию антивирусной защиты сетевого компьютера.

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

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

28. Раскройте цели и задач криптографии как научной области. Перечислите основные направления использования криптографических методов для защиты информации. Нужна ли подобная защита в образовательных организациях? Ответ аргументируйте.

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

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

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

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

33. Опишите программные средства шифрования данных. Раскройте технологию шифрования на примере конкретного приложения.

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

35. Раскройте суть идентификация и аутентификация при входе в информационную систему образовательной организации. Сформулируйте рекомендации по использованию парольных схем. Укажите их возможные недостатки.

36. Раскройте суть электронной цифровой подписи. Охарактеризуйте правовой и технический аспекты. Сформулируйте рекомендации для использования электронной цифровой подписи в образовательных организациях.

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

38. Раскройте понятие «сетевой атаки». Приведите примеры сетевых атак на компьютерную сеть образовательной организации. Укажите пути противодействия сетевым атакам.

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

40. Опишите принципы организации DoS- и DoSS- атак. Расскажите о способах борьбы данным видом информационной угрозы. Возможна ли подобная атака на компьютерные сети образовательных организаций?

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

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

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

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

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

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

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

48. Раскройте суть социальной инженерии. Опишите ее методы.

49. Раскройте сущность электронной наличности. Приведите примеры возможной потери электронных денег при совершении платежей в сети Интернет. Возможна ли оплата электронными деньгами в образовательной организации?

50. Приведите примеры мошенничества в сети Интернет. Раскройте способы противодействия Интернет-мошенникам в сфере образования.

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

Промежуточная аттестация проводится в форме зачета и экзамена, которые служат формой проверки усвоения учебного материала практических занятий, готовности к практической деятельности.

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

Устный ответ на зачете и экзамене

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

3. Котова, Л. В. Сборник задач по дисциплине «Методы и средства защиты информации» [Электронный ресурс] : учебное пособие / Л. В. Котова ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Московский педагогический государственный университет». – Москва : МПГУ, 2015. – 44 с. – Режим доступа :http://biblioclub.ru/index.php?page=book&id=469877

4. 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

Дополнительная литература

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

2. Сагдеев, К.М. Физические основы защиты информации : учебное пособие / К.М. Сагдеев, В.И. Петренко, А.Ф. Чипига ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2015. – 394 с. : ил. – URL: http://biblioclub.ru/index.php?page=book&id=458285. – Библиогр.: с. 387-388. – Текст : электронный.

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

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/
2. http://all-ib.ru - Информационная безопасность. Защита информации
3. http://www.securrity.ru - SecuRRity.Ru — « Информационная безопасност компьютерных систем и защита конфиденциальных данных»
4. 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;

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

– выучите определения терминов, относящихся к теме;

– продумайте примеры и иллюстрации к ответу по изучаемой теме;

– продумывайте высказывания по темам, предложенным к лабораторному занятию.

Рекомендации по работе с литературой:

– ознакомьтесь с аннотациями к рекомендованной литературе и 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 итоговой аттестации;

– 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 информационных справочных систем (обновление выполняется еженедельно)

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

12.2 Перечень современных профессиональных баз данных

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

Оснащение аудиторий

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

аттестации.

Помещение укомплектовано специализированной мебелью и техническими средствами обучения.

Основное оборудование:

Наборы демонстрационного оборудования: автоматизированное рабочее место в составе (учебный мультимедийный комплекс трибуна, гарнитура, проектор, интерактивная доска), магнитно-маркерная доска.

Учебно-наглядные пособия:

Презентации.

Лаборатория вычислительной техники.

Помещение укомплектовано специализированной мебелью и техническими средствами обучения.

Основное оборудование:

Наборы демонстрационного оборудования: автоматизированное рабочее место в составе (системный блок, монитор, клавиатура, мышь), интерактивный дисплей.

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

Учебно-наглядные пособия:

Презентации.

Помещение для самостоятельной работы.

Помещение 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 (персональный компьютер 10 шт.).

Учебно-наглядные пособия:

Презентации.

Читальный зал.

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 10 шт., проектор с экраном 1 шт., многофункциональное устройство 1 шт., принтер 1 шт.)

Учебно-наглядные пособия:

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

Стенды с тематическими выставками..