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): Защита информации в компьютерных сетях

Уровень ОПОП: Бакалавриат

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

Профиль подготовки: Физика. Информатика

обучения: Очная

Разработчики:
Зубрилин А. А., канд. филос. наук, доцент
Кудряшов В.И., канд. пед. наук, доцент.

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

Зав. кафедрой_____Вознесенская Н. В.

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

Зав. кафедрой_____  _Зубрилин А.А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины - формирование навыков организации безопасной работы на персональном компьютере и в компьютерной сети, умений противостоять информационным угрозам, включая технические, технологические, психологические, социальные.

Задачи дисциплины:

– формирование знаний в области российского правового регулирования информационной безопасности;;

– выработка представлений о способах обеспечения защиты компьютера и противостоянии методам социальной инженерии;;

– освоение программных средств обеспечения информационной без-опасности при работе на персональном компьютере и в компьютерной сети, включая формирование умений аргументированного выбора и самостоятельной установки соответствующего программного обеспечения;;

– обучение основам криптографии как одного из важных средств шифрования данных;.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина Б1.В.ДВ.13.01 «Защита информации в компьютерных сетях» относится к вариативной части учебного плана.

Дисциплина изучается на 4 курсе курсе, в 7 семестре.

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):

Компьютерные сети; Интернет технологии;

История и методология информатики и вычислительной техники.

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).

Освоение дисциплины готовит к работе со следующими объектами профессиональной деятельности:

- обучение;
- воспитание;
- развитие.

В процессе изучения дисциплины студент готовится к видам профессиональной деятельности и решению профессиональных задач, предусмотренных ФГОС ВО и учебным планом.

3. Требования к результатам освоения дисциплины

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

Выпускник должен обладать следующими профессиональными компетенциями (ПК):

ПК-2 способностью использовать современные методы и технологии обучения и диагностики педагогическая деятельность	
ПК-2 способностью использовать современные	знать: - понятия, связанные с научной областью «Информационная безопасность»; - возможные технические, технологические, социальные угрозы,

методы и технологии обучения и диагностики	связанные с компьютерной техникой; - меры соблюдения информационной безопасности при работе на компьютере; - виды информационных угроз, возникающих при работе в компьютерных сетях; - программные средства и сервисы Интернет для обеспечения информа-ционной безопасности компьютера; - способы шифрования данных; - правовые и законодательные акты в области обеспечения информационной безопасности; уметь: - аргументировано выбирать и эффективно использовать программные средства для обеспечения информационной безопасности компьютера; - определять оптимальный набор программных средств для обеспечения безопасной работы на компьютере; владеть: - средствами обеспечения информационной безопасности при работе за персональным компьютером и в компьютерных сетях.
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: - возможные технические, технологические, социальные угрозы, связанные с компьютерной техникой; - способы шифрования данных; уметь: - обнаруживать вредоносное программное обеспечение на компьютере и выявлять сетевые атаки; - устранять последствия воздействия на компьютер вредоносного программного обеспечения и сетевых атак; - аргументировано выбирать и эффективно использовать программные средства для обеспечения информационной безопасности компьютера; - определять оптимальный набор программных средств для обеспечения безопасной работы на компьютере; - применять программы для шифрования конфиденциальной информации; владеть: - средствами обеспечения информационной безопасности при работе за персональным компьютером и в компьютерных сетях.

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Седьмой семестр
Контактная работа (всего)	**36**	**18**
Лабораторные	36	18
Самостоятельная работа (всего)	**72**	**72**
Виды промежуточной аттестации		
Зачет		+
Общая трудоемкость часы	**108**	**108**
Общая трудоемкость зачетные единицы	**3**	**3**

5. Содержание дисциплины

5.1. Содержание модулей дисциплины

Модуль 1. Правовые вопросы защиты информации в компьютерных сетях:

Общие вопросы информационной безопасности. Международные стандарты информационного обмена. Понятие информационной угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». Нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Закон об информации. Судебные прецеденты и ответственность за нарушение закона. Концепция информационной безопасности РФ. Информационная безопасность личности, общества, государства.

Теория информационной безопасности и ее основные направления. Ведущие положения теории информационной безопасности в области информационных систем. Модели безопасности и их применение. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

Виды возможных нарушений информационной безопасности. Несформированность информационной культуры пользователей. Хакерские атаки. DoS- и DDoS- атаки. Сетево шпионаж (сниффинг, нюкеры). Эксплойты.

Причины возникновения информационных угроз. Анализ способовнарушения информационной безопасности. Использование защищенных компьютерных систем.

Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

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

Программные и аппаратные средства, связанные с угрозой обеспечения информационной безопасности.

DoS- и DDoS- атаки как инструмент ограничения доступа к сетевому компьютеру. Комплексная защита сетевого компьютера от информационных угроз. Брандмауэр как аппаратное и программное средство ограничения доступа к информации. Программные средства компьютера по обнаружению вторжения и защите от него.

Модуль 2. Программные средства и сервисы сети Интернет по защите информации: Понятие о видах вирусов. Антивирусная защита компьютера. Классификация компьютерных вирусов. Классические компьютерные вирусы. Файловые вирусы. Макровирусы. Троянские кони. Руткиты. Сетевые черви. Программные средства для обеспечения антивирусной защиты компьютера.

Технологии построения защищенных информационных систем. Место информационной безопасности экономических систем в национальной безопасности страны. Риски и ценностьинформации.

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

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

Антивирусные программные средства офисного и домашнего назначения для обеспечения информационной безопасности.

Парольная защита. Программы шифрования данных Социальная инженерия и ее методы.

Электронная валюта

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

5.2. Содержание дисциплины: Практические (36 ч.)

Модуль 1. Проблемы информационной безопасности в современном обществе (18 ч.)

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

Общие вопросы информационной безопасности. Информационные ресурсы по информационной безопасности.

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

Правовое регулирование в области информационной безопасности.

Законы о преступлениях в сфере информационных технологий.

Авторское право. Пути доказательства авторства.

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

Интеллектуальная собственность. Способы защиты интеллектуальной собственности. Лицензионное программное обеспечение.

Компьютерное пиратство и законодательная ответственность за него.

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

Государственная тайна. Ответственность за разглашение государственной тайны. Состояние законодательства РФ в области сохранения государственной тайны.

Примеры нарушения государственной тайны.

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

Несанкционированный доступ к аппаратным средствам компьютера и средства ограничения доступа.

Взлом экранной заставки Windows и пароля BIOS. Способы предотвращения взлома. Взлом операционной системы посредством носителей информации. Способы защиты. Ограничение доступа к USB-накопителям.

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

Тема 6. DoS- и DDoS- атаки как инструмент ограничения доступа к сетевому 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 Сайтыс 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 2. Проблемы информационной безопасности в современном обществе (18 ч.)

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

Вредоносное программное обеспечение и пути его попадания в компьютер пользователя. Компьютерная реклама как инструмент заражения компьютера. Руткиты.

Клавиатурные шпионы (кейлоггеры).

Функциональные возможности антивирусных программных средств.

Онлайн антивирусы

Sms-блокеры и методы борьбы с ними.

Тема 11. Парольная защита (2 ч.)

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

Хранители паролей.

Программы восстановления (взлома) паролей. Брутфорс

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

Обзор методов социальной инженерии.

Методы и методики психологического воздействия на личность (универсальный сеанс связи, сообщение о проверке почты, сообщение от имени администратора, квитанция о доставке, обличение и др.).

Антропогенные инструменты защиты от методов социальной инженерии (привлечение к вопросам безопасности, изучение и внедрение необходимых методов и действий для повышения защиты информационного обеспечения).

Обратная социальная инженерия.

Тема 13. Социальная инженерия и ее методы (2 ч.)

Фарминг как инструмент скрытого перенаправления на поддельные сайты. Фишинг и вишинг как инструмент получения конфиденциальной информации. Мошенничество в Интернете.

Правила поведения пользователей в сети Интернет при работе с информационными ресурсами.

Тема 14. Программы шифрования данных (2 ч.)

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

Криптография и ее методы шифрования информации.

Восстановление данных. Грамотное удаление информации с компьютера. Специализированные программные средства по удалению.

Тема 15. Электронная валюта (2 ч.)

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

Проблемы электронной оплаты. Способы заработка в Интернете.

Тема 16. Социальные сети как информационная угроза (2 ч.) Социальная сеть как инструмент сбора информации о гражданине. Инициируемые и не инициируемые пользователем угрозы в социальных сетях. Меры защиты от информационных угроз в социальной сети.

Тема 17. Фильтрация сетевого контента (2 ч.)

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

Тема 18. Политика информационной безопасности и ее организация в локальной сети (2 ч.)

Настройка безопасности групповой работы с информационными ресурсами в локальной сети. Локальная политика безопасности. Авторизация и ее задачи.

Настройка аудита сетевых ресурсов. Работа с журналом безопасности.

Защита локальной сети от взлома. Сниффинг.

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

6.1 Вопросы и задания для самостоятельной работы

Седьмой семестр(72 ч.)

Модуль 1. Правовые вопросы защиты информации в компьютерных сетях (36 ч.)

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. Практические вопросы организации информационной безопасности в компьютерных сетях (36 ч.)

Вид СРС: *Выполнение индивидуальных заданий

СХЕМА ОФОРМЛЕНИЯ ОПИСАНИЯ ПРИЛОЖНЕНИЯ ДЛЯ ОРГАНИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА КОМПЬЮТЕРЕ

Общие сведения (20 баллов) Название приложения:

Производитель:

Сайт производителя:

Необходимость инсталляции (да/нет)

Требования к операционной системе и аппаратным ресурсам ПК:

Обновление (ручное/автоматическое)

Тип приложения (бесплатное, условно-бесплатное, лицензионное) Функциональные возможности:

Описание приложения (35 баллов) Скриншот приложения

Описание пунктов меню приложения Настройка приложения (45 баллов) Описание настройки приложения на работу

Описание этапов работы с приложением по обеспечению информационной безопасности на компьютере

Список приложений для рассмотрения

Межсетевые экраны (со встроенным и без встроенного антивируса)

AVG Internet Security

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

7. Тематика курсовых работ(проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

8. Оценочные средства для промежуточной аттестации

8.1. Компетенции и этапы формирования

Коды компетенций	Этапы формирования		
	Курс, семестр	Форма контроля	Модули (разделы) дисциплины
ПК-2	4 курс, Седьмой семестр	Зачет	Модуль 1: Проблемы информационной безопасности в современном обществе

ПК-4	4 курс, Седьмой семестр	Зачет	Модуль 2: Практические вопросы организации информационной безопасности в компьютерных сетях

Компетенция ПК-2 формируется в процессе изучения дисциплин:

Естественнонаучная картина мира, Защита информации в компьютерных сетях, Информационная безопасность в образовании, Информационные технологии в физических исследованиях, Компьютерная обработка результатов физических исследований, Методика и техника школьного физического эксперимента, Методика обучения информатике, Методика обучения физике, Педагогическая практика, Практика по получению профессиональных умений и опыта профессиональной деятельности, Преддипломная практика, Разработка приложений в Microsoft Visual Studio, Русский язык и культура речи, Школьный кабинет физики.

Компетенция ПК-4 формируется в процессе изучения дисциплин:

Волновые свойства света, Естественнонаучная картина мира, Законы геометрической оптики, Защита информации в компьютерных сетях, Интернет-технологии, Информационная безопасность в образовании, Квантовая физика, Компьютерные сети, Методика и техника школьного физического эксперимента, Методика обучения информатике, Механика, Молекулярная физика и термодинамика, Оптика, Педагогическая практика, Практика по получению профессиональных умений и опыта профессиональной деятельности, Преддипломная практика, Теоретические основы информатики, Технические средства обучения, Школьный кабинет физики, Электричество и магнетизм.

8.2. Показатели и критерии оценивания компетенций, шкалы оценивания

В рамках изучаемой дисциплины студент демонстрирует уровни овладения компетенциями:

Повышенный уровень:

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

Базовый уровень:

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

Пороговый уровень:

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

Уровень ниже порогового:

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

Уровень сформированности компетенции	Шкала оценивания для промежуточной аттестации	Шкала оценивания по БРС
	Зачет	
Повышенный	зачтено	90 – 100%
Базовый	зачтено	76 – 89%

Пороговый	зачтено	60 – 75%
Ниже порогового	не зачтено	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.

8.3. Вопросы, задания текущего контроля

Модуль 1: Правовые вопросы защиты информации в компьютерных сетях

ПК-2 способностью использовать современные методы и технологии обучения и диагностики

1. Изучите нормативную базу, регламентирующую организацию информационной безопасности при работе в компьютерных сетях.

2. Рассмотрите Концепцию информационной безопасности РФ.

3. Проанализируйте методические материалы по организации безопасной работы за компьютерами на предприятии.

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

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

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. Проанализируйте файлообменные системы на пердмет наличия приложений по организации инофрмационной безопасности.

2. Изучите вопрос установки специализированных приложений по обеспечению информационной безопасности на компьютере.

3. Рассмотрите технологию выбора программных продуктов для обеспечения 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.

8.4. Вопросы промежуточной аттестации

Седьмой семестр (Зачет, ПК-2, 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.

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

4 Дайте определение государственной тайны. Перечислите основные статьи в Федеральном Законе о государственной тайне.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

20 Охарактеризуйте организационные меры защиты информации на предприятии.

Обоснуйте основные мероприятия по обеспечению информационной безопасности.

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

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

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

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

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

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

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

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 служит 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.

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. Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях [Электронный ресурс] : учебное пособие / А. М. Голиков ; Министерство образования и науки

Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). – Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=480637

2. Мэйволд, Э. Безопасность сетей [Электронный ресурс] / Э. Мэйволд. – 2-е изд., испр. – М. : Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с. – Режим доступа :

//biblioclub.ru/index.php?page=book&id=429035

3.Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О. В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». – Самара : Самарский государственный архитектурно-строительный университет, 2014. – 113 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=438331

4. 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

5. 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

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

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, коврик), проектор, экран, интерактивная доска, магнитно-маркерная доска, колонки SVEN, наушники.

Учебно-наглядные пособия:

Презентации.

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

Учебно-наглядные пособия:

Презентации.

Помещения для самостоятельной работы.

Лаборатория вычислительной техники.

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.).

Учебно-наглядные пособия:

Презентации.

Помещение для самостоятельной работы.

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..