Подписано электронной подписью:
Вержицкий Данил Григорьевич
Должность: Директор КГПИ ФГБОУ ВО «КемГУ»
Дата и время: 2024-02-21 00:00:00
471086fad29a3b30e244e72babc56b1ab55c9d5024dde10e75e03a5b6fdf6436

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кемеровский государственный университет»
Новокузнецкий институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования
«Кемеровский государственный университет»

Факультет физико-математический и технолого-экономический
Профилирующая кафедра теории и методики преподавания информатики

УТВЕРЖДАЮ
Декан ФМ и ТЭФ
_____ И.И. Тимченко
«24» марта 2017г.

Рабочая программа дисциплины (модуля)
Б1.В.ДВ.13.1 Методы и средства защиты информации

Направление подготовки
44.03.01 Педагогическое образование

Направленность (профиль) подготовки
Информатика

Программа: ***академический бакалавриат***

Квалификация (степень) выпускника
бакалавр

Форма обучения
заочная

Год набора 2016

Новокузнецк, 2017

Лист внесения изменений

Сведения об утверждении:
утверждена Ученым советом факультета
(протокол Ученого совета факультета № _6_ от _3_.03__.2016_)
на 20_16___ год
Одобрена на заседании методической комиссии
протокол методической комиссии факультета № _6_ от 18._02_.2016_)
Одобрена на заседании обеспечивающей кафедры
протокол № _7_ от 16._03_.2016_) М.С.Можаров *(Ф. И.О. зав. кафедрой)* / _____ *(подпись)*

Изменения по годам:
На 2017_ год

утвержден (а) Ученым советом факультета
(протокол Ученого совета факультета № 7 от 16.03.2017)
на 2017 год набора
Одобрен (а) на заседании методической комиссии
протокол методической комиссии факультета № 7 от 15.03.2017)
Одобрен (а) на заседании обеспечивающей кафедры ТиМПИ
протокол № 8 от 02.03.2017) Можаров М.С. (Ф. И.О. зав. кафедрой) / _____ (подпись)

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

2. Место дисциплины в структуре ООП

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

3.1. Объём дисциплины (модуля) по видам учебных занятий (в часах)

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкость по видам учебных занятий (в академических часах)

4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

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

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

6.1. Паспорт фонда оценочных средств по дисциплине (модулю)

6.2. Типовые контрольные задания или иные материалы

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

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

а) основная учебная литература:

б) дополнительная учебная литература:

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), необходимых для освоения дисциплины (модуля)

9. Методические указания для обучающихся по освоению дисциплины (модуля)

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

12. Иные сведения и (или) материалы

12.1. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

12.2 Занятия, проводимые в интерактивных формах

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения основной образовательной программы «Педагогическое образование» по профилю "Информатика"

В результате освоения ООП бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине (модулю):

Коды компетенции	**Результаты освоения ООП** ***Содержание компетенций***	**Перечень планируемых результатов обучения по дисциплине**
ОПК-4	готовностью к профессиональной деятельности в соответствии с нормативно-правовыми актами сферы образования	Знать: приоритетные направления развития образовательной системы Российской Федерации; базовые нормативно-правовые акты сферы образования, нормативные документы по вопросам обучения и воспитания детей и молодежи; законодательство о правах ребенка; Конвенцию о правах ребенка. Уметь: анализировать нормативно-правовые акты, регулирующие профессиональную деятельность педагога, в том числе документы, регламентирующие защиту достоинства и интересов обучающихся, помощь детям, оказавшимся в конфликтной ситуации и/или неблагоприятных условиях; планировать свою деятельность в соответствии с нормами образовательного законодательства. Владеть: способами решения педагогических задач, требующих принятия правовых мер по защите прав обучающегося; навыками соблюдения правовых, нравственных и этических норм, требований профессиональной этики в условиях реальных педагогических ситуаций.

2. Место дисциплины в структуре ООП бакалавриата

Дисциплина «Методы и средства защиты информации» относится к вариативной части профессионального цикла дисциплин (Б3.В.ДВ.10).

Для освоения дисциплины «Методы и средства защиты информации» студенты используют знания, умения, навыки, сформированные в процессе изучения студентами математических и информационно-технологических дисциплин, а также практический опыт работы с вычислительной техникой.

Дисциплина (модуль) изучается на __2 курсе (ах) в __4__ семестре.

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины (модуля) составляет __3__ зачетных единиц (ЗЕТ), ___108_____ академических часа.

3.1. Объём дисциплины (модуля) по видам учебных занятий (в часах)

Объём дисциплины	**Всего часов**	
	для очной формы обучения	для заочной /очно-заочной формы обучения
Общая трудоемкость дисциплины	108	108

Объём дисциплины	Всего часов	
	для очной формы обучения	для заочной /очно-заочной формы обучения
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	36	8
Аудиторная работа (всего**):	36	8
в т. числе:		
Лекции	18	4
Семинары, практические занятия		
Практикумы		
Лабораторные работы	18	4
Занятия в интерактивной форме	10	2
Внеаудиторная работа (всего**):	36	91
В том числе, индивидуальная работа обучающихся с преподавателем:		
Курсовое проектирование		
Групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем		
Творческая работа (эссе)		
Самостоятельная работа обучающихся (всего)	36	91
Вид промежуточной аттестации обучающегося (зачет / экзамен)	Экзамен, 36	Экзамен, 9

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкость по видам учебных занятий (в академических часах)

для очной формы обучения

№ п/п	Раздел дисциплины	Общая трудоёмкость *(часах)*	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			Формы текущего контроля успеваемости
			аудиторные учебные занятия		самостоя-тельная работа обучаю-щихся	
		всего	лекции	семинары, практи-ческие занятия		
1.	Основные понятия информационной безопасности систем. Источники атак на информацию, риски.	8	2	2	4	Устный опрос, лаборатор-ная работа
2.	Политика	8	2	2	4	Устный

№ п/п	Раздел дисциплины	Общая трудоёмкость *(часах)*	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			Формы текущего контроля успеваемости
			аудиторные учебные занятия		самостоя-тельная работа обучаю-щихся	
		всего	лекции	семинары, практи-ческие занятия		
	безопасности. Стандарты безопасности.					опрос, лаборатор-ная работа
3.	Криптографические модели. Алгоритмы шифрования.	10	2	2	6	Тест, лаборатор-ная работа
4.	Модели безопасности основных ОС.	8	2	2	4	Тест, лаборатор-ная работа
5.	Алгоритмы аутентификации пользователей.	8	2	2	4	Тест, лаборатор-ная работа
6.	Многоуровневая защита корпоративных сетей.	12	4	4	4	Тест, лаборатор-ная работа
7.	Защита информации в сетях.	10	2	2	6	Тест, лаборатор-ная работа
8.	Требования к системам защиты информации.	8	2	2	4	Тест, лаборатор-ная работа

для заочной (очно-заочной) формы обучения

№ п/п	Раздел дисциплины	Общая трудоёмкость *(часах)*	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			Формы текущего контроля успеваемости
			аудиторные учебные занятия		самостоятельная работа обучающихся	
		всего	лекции	семинары, практические занятия		
1.	Основные понятия информационной безопасности систем.	12	1	1	10	Устный опрос, лабораторная работа

№ п/п	Раздел дисциплины	Общая трудоёмкость *(часах)*	Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)			Формы текущего контроля успеваемости
			аудиторные учебные занятия		самостоятельная работа обучающихся	
		всего	лекции	семинары, практические занятия		
	Источники атак на информацию, риски.					
2.	Политика безопасности. Стандарты безопасности.	16	1	1	14	Устный опрос, лабораторная работа
3.	Криптографические модели. Алгоритмы шифрования.	20	1	1	18	Тест, лабораторная работа
4.	Модели безопасности основных ОС. Алгоритмы аутентификации пользователей.	16	1	1	14	Тест, лабораторная работа
5.	Защита информации в сетях.	19	1	1	17	Тест, лабораторная работа
6.	Требования к системам защиты информации.	16	1	1	14	Тест, лабораторная работа

4.2 Содержание дисциплины (модуля), структурированное по темам (разделам)

№ п/п	Наименование раздела дисциплины	Содержание
Содержание лекционного курса		
1	Основные понятия информационной безопасности систем. Источники атак на информацию, риски.	Основные понятия информационной безопасности (ИБ) систем. Источники, риски и формы атак на информацию. Международные стандарты информационного обмена. Понятие угрозы. Необходимость защиты информационных систем и телекоммуникаций. Основные задачи обеспечения защиты информации.
2	Политика безопасно	Политика безопасности. Стандарты безопасности. Анализ

№ п/п	Наименование раздела дисциплины	Содержание
	ти. Стандарты безопасности.	угроз ИБ. Классификация видов угроз ИБ по различным признакам. Свойства информации: конфиденциальность, доступность, целостность. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз ИБ.
3	Криптографические модели. Алгоритмы шифрования.	Криптографические модели. Алгоритмы шифрования.
4	Модели безопасности основных ОС.	Модели безопасности основных ОС. Особенности современных информационных систем, факторы влияющие на безопасность информационной системы. Понятие информационного сервиса безопасности. Виды сервисов безопасности. Идентификация и аутентификация. Парольные схемы аутентификации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом).
5	Алгоритмы аутентификации пользователей.	Алгоритмы аутентификации пользователей. Использование криптографических средств для решения задач идентификация и аутентификация. Электронная цифровая подпись (ЭЦП), принципы ее формирования и использования. Подтверждение подлинности объектов и субъектов информационной системы.
6	Многоуровневая защита корпоративных сетей.	Многоуровневая защита корпоративных сетей. Основные нормативные руководящие документы, нормативно-справочные документы. Задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Концепция информационной безопасности.
7	Защита информации в сетях.	Защита информации в сетях. Критерии безопасности компьютерных систем министерства обороны США (“Оранжевая книга”). Базовые требования безопасности: требования политики безопасности, требования подотчетности (аудита), требования корректности. Классы защищенности компьютерных систем. Интерпретация и развитие Критериев безопасности.
8	Требования к системам защиты информации.	Требования к системам защиты информации. Иерархический метод разработки защищенных систем. Структурный принцип. Принцип модульного программирования. Исследование корректности реализации и верификации автоматизированных систем. Спецификация требований предъявляемых к системе. Основные этапы разработки защищенной системы.
Темы лабораторных занятий		
1	Криптографические методы защиты.	Реализация криптографического преобразования информации по одному из доступных алгоритмов.
2	Алгоритмы	Изучение принципов аутентификации пользователей веб-

№ п/п	Наименование раздела дисциплины	Содержание
	аутентификации пользователей.	сервисов.
3	Модели безопасности основных ОС.	Определение наличия и удаление вредоносного ПО с помощью программных средств антивирусного ПО.
4	Многоуровневая защита корпоративных сетей.	Исследование механизмов парольной защиты, методов противодействия атакам на пароль.
5	Защита информации в сетях.	Управление правами доступа к ресурсам ОС, ИС и веб-сервисов.
6	Требования к системам защиты информации.	Развертывание веб-сервера. Настройка параметров безопасности. Испытания эффективности его защиты.

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

Темы для рефератов:

1. Вредоносное ПО: способы распространения, опасность, методы защиты.
2. Программные закладки: типы, способы внедрения и защиты.
3. Аппаратные средства защиты информации.
4. Сравнительный анализ средств защиты электронной почты.
5. Сравнительный анализ систем обнаружения атак.
6. Сравнительный анализ межсетевых экранов.
7. Анализ методов изучения поведения нарушителей безопасности компьютерных систем.
8. Анализ методов нарушения безопасности сетевых ОС и методов противодействия им.
9. Применение биометрической информации для аутентификации пользователей компьютерных систем.
10. Стандарты безопасности компьютерных систем и информационных технологий.
11. Сравнительный анализ методов и программных средств защиты от спама.
12. Методы и программные средства перехвата и анализа контента.
13. Уязвимости симметричных и асимметричных криптографических систем.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

6.1. Паспорт фонда оценочных средств по дисциплине (модулю)

№ п/п	Контролируемые разделы (темы) дисциплины (результаты по разделам)	Код контролируемой компетенции* (или её части)	наименование оценочного средства
1.	Методы защиты информации	ОПК-4	Тест
2.	Требования к	ОПК-4	Тест

№ п/п	Контролируемые разделы (темы) дисциплины (результаты по разделам)	Код контролируемой компетенции* (или её части)	наименование оценочного средства
	системам защиты информации.		
3.	Модели безопасности основных ОС. Алгоритмы аутентификации пользователей.	ОПК-4	Тест

6.2. Типовые контрольные задания или иные материалы

6.2.1. Экзаменационный тест

1. Укажите три основные угрозы для информации в человеко-компьютерных системах:
   a. Резервное копирование
   b. Сбои оборудования
   c. Протоколирование состояния системы
   d. Случайная утрата или изменение
   e. Преднамеренное искажение
   f. Санкционированный просмотр

2. В эталонной модели OSI, шифрование входит в функции уровня...
   a. Канального (2)
   b. Сетевого (3)
   c. Сеансового (5)
   d. Представления (6)
   e. Транспортного (4)
   f. Физического (1)
   g. Приложений (7)

3. Вредоносный код обладает следующими чертами: не требует программы-носителя, самовоспроизводится и размножается по сети без ведома пользователя, заражая другие компьютеры. Его тип -
   a. Червь
   b. Троянский конь
   c. Файловый вирус
   d. Макровирус

4. Наиболее опасной из приведенных процедур восстановления забытого пароля является...
   a. пересылка текущего пароля на адрес электронной почты, при этом адрес заполняется автоматически из профиля заявителя
   b. пересылка на адрес электронной почты, связанной с профилем, ссылки на процедуру восстановления пароля, имеющую ограниченный срок актуальности
   c. пересылка текущего пароля на адрес электронной почты, при этом адрес и логин указывается вручную заявителем
   d. генерация нового пароля и его пересылка на адрес электронной почты, указанной в профиле заявителя

5. Межсетевые экраны служат для
   a. Изоляции некоторой сети от других с помощью настраиваемых фильтров трафика и/или анализаторов угроз

b. сбора статистики использования каналов связи сотрудниками организации
c. Для просмотра информации, распределенной по узлам нескольких сетей
d. подтверждения подлинности сообщений, принятых по сети
e. отображения информации о состоянии сети

6. Криптосистема обладает следующими чертами: предусматривает использование открытого ключа для шифрования и закрытого для дешифрования данных. Тип криптосистемы -
a. Избыточная
b. Симметричная
c. Асиметричная
d. С использованием инфраструктуры открытых ключей (PKI)

7. Среди методов защиты информации от ошибочных действий пользователей можно выделить три наиболее эффективных:
a. Резервирование носителей информации
b. Автоматический запрос на подтверждение выполнения команды или операции
c. Шифрование файлов
d. Предоставление возможности отмены последнего действия
e. Установление специальных атрибутов файлов
f. Отчет о действиях пользователя

8. Под целостностью в контексте информационной безопасности понимают
a. возможность за приемлемое время получить требуемую информационную услугу
b. актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения
c. полноту предоставляемых данных по теме запроса
d. комплексный подход к обеспечению информационной безопасности

9. Наиболее частыми и опасными угрозами ИБ являются
a. непреднамеренные ошибки штатных пользователей, операторов или администраторов ИС
b. хакерские атаки
c. сбои аппаратного обеспечения и поддерживающей инфраструктуры
d. стихийные бедствия, забастовки, войны

10. Протокол удаленного администрирования, аналогичный Telnet, но обеспечивающий шифрование потока данных, а также различные варианты аутентификации:
a. SSH
b. VPN
c. RDP
d. TLS
e. SSL

11. Три наиболее важных метода защиты информации от несанкционированного доступа:
a. Архивирование (создание резервных копий)
b. Регулярное обновление аппаратных средств
c. Шифрование информации
d. Установка паролей на доступ к информации
e. Использование антивирусных программ

12. Окном опасности называют
a. диалоговое окно ОС или антивирусной программы с предупреждением об опасности

b. средства, используемые злоумышленниками для установки средств удаленного управления компьютером

c. уязвимости в защите ПО или ИС, позволяющие создать угрозу информационной безопасности

d. промежуток времени от момента, когда появляется возможность использовать уязвимость в защите, и до момента, когда она ликвидируется

13. Согласно стандарту Министерства обороны США "Критерии оценки доверенных компьютерных систем" (известным под названием "Оранжевая книга") степень доверия системе оценивается по двум основным критериям:

a. Степень квалификации пользователей
b. Стоимость систем обеспечения безопасности
c. Политика безопасности
d. Уровень гарантированности
e. Квалификации сотрудников физической охраны

14. Электронная цифровая подпись (ЭЦП) ...

a. это подпись под сообщением или документом, включающая контакты отправителя
b. ставится на сенсорном экране
c. применяется только для обмена служебными документами, но не личной информацией
d. предназначена для защиты электронного документа от подделки
e. это скан рукописной личной подписи

15. Монитор обращений ("ядро безопасности") должен обладать как минимум тремя важными характеристиками:

a. Документированность
b. Изолированность
c. Полнота
d. Прозрачность
e. Верифицируемость

16. Криптосистема обладает следующими чертами: предусматривает использование одного и того же закрытого ключа для шифрования и дешифрования данных, характеризуется высокой скоростью работы, но сложностью передачи самого этого закрытого ключа. Тип криптосистемы -

a. С использованием инфраструктуры открытых ключей (PKI)
b. Избыточная
c. Асиметричная
4. Симметричная

17. Предоставление полномочий на выполнение определенных действий в некоторой информационной системе называется...

a. аутентификацией
b. мандатным контролем доступа
c. авторизацией
d. инагурацией
e. идентификацией

18. При реализации механизмов безопасности при сетевом соединении, наибольшее число таких механизмов можно реализовать на следующем уровне модели OSI:

a. Физический (1)

b. Сеансовый (5)
c. Сетевой (3)
d. Транспортный (4)
e. Презентативный (6)
f. Прикладной (7)
g. Канальный (2)

19. Протокол передачи данных, обеспечивающий шифрование потока данных на транспортном уровне:
a. TCP
b. SSL
c. RDP
d. SSH
e. VPN

20. Вредоносный код обладает следующими чертами: распространяется как часть приложения, нередко имеющего привлекательный функционал (игры, программы для взлома и т.п.), что стимулирует его загрузку и запуск самим пользователем. Его тип -
a. Троянский конь
b. Червь
c. Файловый вирус
d. Макровирус

21. Доступностью в терминах информационной безопасности называется
a. возможность за приемлемое время получить требуемую информационную услугу
b. информация, изложенная доступным для понимания образом
c. актуальность и непротиворечивость информации
d. полная открытость всех информационных объектов для любых пользователей

22. Под конфиденциальностью в контексте информационной безопасности понимают
a. актуальность и непротиворечивость информации
b. защиту информации от несанкционированного доступа
c. механизм управления паролями доступа к ИС
d. степень доверия к получаемой информации

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

а) основная учебная литература:

1. Башлы П. Н. Информационная безопасность и защита информации: Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. ISBN 978-5-369-01178-2. Доступ: http://znanium.com/catalog.php?bookinfo=405000

2. Бирюков А.А. Информационная безопасность: защита и нападение. – М.: ДМК Пресс, 2012. – 474 с.: ил. ISBN 978-5-94074-647-8. Доступ: http://e.lanbook.com/books/element.php?pl1_id=39990

3. Шаньгин В.Ф. Информационная безопасность. – М.: ДМК Пресс, 2014. – 702 с.: ил. ISBN 978-5-94074-768-0. Доступ: http://e.lanbook.com/books/element.php?pl1_id=50578

б) дополнительная учебная литература:

1. Бабаш А.В. Криптографические методы защиты информации. Том 3: Учебно-методическое пособие. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с. ISBN 978-5-369-01304-5. Доступ: http://znanium.com/catalog.php?bookinfo=432654

2. Баранова Е.К., Бабаш А.В. Моделирование системы защиты информации: Практикум: Учебное пособие. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 - 120 с. ISBN 978-5-369-01379-3. Доступ: http://znanium.com/catalog.php?bookinfo=476047

3. Гвоздева В.А., Лаврентьева И.Ю. Основы построения автоматизированных информационных систем: Учебник. - М.: ИД ФОРУМ: НИЦ Инфра-М, 2013. - 320 с.: ил. ISBN 978-5-8199-0315-5. Доступ: http://znanium.com/catalog.php?bookinfo=392285

4. Кнауб Л. В. Теоретико-численные методы в криптографии: Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. ISBN 978-5-7638-2113-7. Доступ: http://znanium.com/catalog.php?bookinfo=441493

5. Корпоративные информационные системы управления: Учебник / Под науч. ред. Н.М. Абдикеева, О.В. Китовой. - М.: ИНФРА-М, 2011. - 464 с. ISBN 978-5-16-004373-9. Доступ: http://znanium.com/catalog.php?bookinfo=200718

6. Партыка Т.Л., Попов И.И. Информационная безопасность: Учебное пособие. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с.: ил. ISBN 978-5-91134-627-0. Доступ: http://znanium.com/catalog.php?bookinfo=420047

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Национальный открытый университет Интуит. –режим доступа http://www.intuit.ru/

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид учебных занятий	Организация деятельности студента
Лекция	Лекции построены на основе использования активных форм обучения: - **лекция-беседа (п**реимущество лекции-беседы состоит в том, что она позволяет привлекать внимание студентов к наиболее важным вопросам темы, определять содержание и темп изложения учебного материала с учетом особенностей студентов), - **проблемная лекция** (с помощью проблемной лекции обеспечивается достижение трех основных дидактических целей: усвоение студентами теоретических знаний; развитие теоретического мышления; формирование познавательного интереса к содержанию учебного предмета и профессиональной мотивации будущего специалиста), **--лекция с заранее запланированными ошибками** (Эта форма проведения лекции необходима для развития у студентов умений оперативно анализировать профессиональные ситуации, выступать в роли экспертов, оппонентов, рецензентов, вычленять неверную или неточную информацию). На каждой лекции применяется сочетание этих форм обучения в зависимости от подготовленности студентов и вопросов, вынесенных на лекцию. Присутствие на лекции не должно сводиться лишь к автоматической записи изложения предмета преподавателем. Более того, современный насыщенный материал каждой темы не может (по времени) совпадать с записью в тетради из-за разной скорости процессов – мышления и автоматической записи. Каждый студент должен разработать для себя систему ускоренного фиксирования на бумаге материала лекции. Поэтому, лектором ***рекомендуется формализация записи*** посредством использования общепринятых логико-математических символов, сокращений,

	алгебраических (формулы) и геометрических (графики), системных (схемы, таблицы) фиксаций изучаемого материала. Овладение такой методикой, позволяет каждому студенту не только ускорить процесс изучения, но и повысить его качество, поскольку успешное владение указанными приемами требует переработки, осмысления и структуризации материала.
Лабораторная работа	Вузовская подготовка специалистов должна обеспечивать приобретение ими не только знаний, но и умений использовать полученные знания на практике. Это требование и положено в основу целей и методов проведения лабораторных работ по вышеуказанной учебной дисциплине. Лабораторные работы предлагаются в соответствии с рабочей программой в рамках каждой темы.
Подготовка к экзамену	Подготовка к экзамену предполагает изучение рекомендуемой литературы и других источников, конспектов лекций, повторение материалов практических занятий.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Тематические презентации, антивирусное ПО, служебные программы диагностики, системы программирования, серверы учебного назначения.

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Для проведения лекционных занятий используется поточная аудитория на 75 мест (с проектором для демонстрации презентаций по всем темам курса), для проведения практических занятий – аудитории на 20 мест.

Для пользования электронными ресурсами используется персональная компьютерная техника с доступом в Интернет.

12. Иные сведения и (или) материалы

12.1. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Особенности реализации программы курса для инвалидов и людей с ограниченными возможностями здоровья зависит от состоянии их здоровья и конкретных проблем, возникающих в каждом отдельном случае.

- При организации образовательного процесса для слабослышащих студентов от преподавателя курса требуется особая фиксация на собственной артикуляции. Говорить следует немного громче и четче.
- На занятиях преподавателю требуется уделять повышенное внимание специальным профессиональным терминам, а также к использованию профессиональной лексики. Для лучшего усвоения слабослышащими специальной терминологии необходимо каждый раз писать на доске используемые термины и контролировать их усвоение.
- В процессе обучения рекомендуется использовать разнообразный наглядный материал. Все лекции курса снабжены компьютерными мультимедийными презентациями.
- В процессе работы со слабовидящими студентами педагогическому работнику следует учитывать, для усвоения информации слабовидящим требуется большее количество повторений и тренировок по сравнению с лицами с нормальным зрением.
- Информацию необходимо представлять в том виде, в каком ее мог бы получить слабовидящий обучающийся: крупный шрифт (16 - 18 пунктов). Следует предоставить возможность слабовидящим использовать звукозаписывающие устройства и компьютеры во время занятий по курсу. При лекционной форме занятий студенту с плохим зрением следует

разрешить пользоваться диктофоном - это его способ конспектировать. Не следует забывать, что все записанное на доске должно быть озвучено.

- В работе с маломобильными обучающимися предусматривается возможность консультаций посредством электронной почты.

12.2 Занятия, проводимые в интерактивных формах

№ п/п	Раздел, тема дисциплины	Объем аудиторной работы в интерактивных формах по видам занятий (час.)			Формы работы
		Лекц.	Практич	Лабор.	
1.	Методы защиты информации	2			Проблемная лекция
2.	Средства защиты информации			4	Работа в малых группах
3.	Требования к системам безопасности			4	Работа в малых группах
	ИТОГО по дисциплине:	2		8	

Составитель (и): Читайло А.И., ст. преподаватель
(*фамилия, инициалы и должность преподавателя (ей)*)

Макет рабочей программы дисциплины (модуля) разработан в соответствии с приказом Минобрнауки России от 19.12.2013 № 1367, одобрен научно-методическим советом (протокол № 8 от 09.04.2014 г.) и утвержден приказом ректора от 23.04.2014 № 224/10..

Макет обновлён с поправками в части подписей на титульной странице, п.3 добавлена строка для указания часов, проводимых в активной и интерактивной формах обучения, добавлен п. 12.1 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья (протокол НМС № 6 от 15.04.2015 г.), утвержден приказом ректора.