Подписано электронной подписью:
Вержицкий Данил Григорьевич
Должность: Директор КГПИ ФГБОУ ВО «КемГУ»
Дата и время: 2024-02-21 00:00:00
471086fad29a3b30e244c728abc3661ab35c9d50210dcf0e75e03a5b6fdf6436

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
Кафедра теории и методики преподавания информатики

УТВЕРЖДАЮ
Декан ФМ и ТЭФ
_____ И.И. Тимченко
«15» февраля 2018г.

Рабочая программа дисциплины (модуля)

__Б1.В.ДВ.9.2_Информациионная безопасность____
Код, название дисциплины /модуля

Направление / *специальность* подготовки
44.03.05 Педагогическое образование (с двумя профилями подготовки)
Код, название направления / специальности

Направленность (профиль) подготовки
_____Математика и Информатика____

Программа академического бакалавриата

Квалификация выпускника
_____бакалавр____
Бакалавр/ магистр / специалист

Форма обучения
_____очная_____
Очная, очно-заочная, заочная

Год набора 2018

Новокузнецк 2018

Лист внесения изменений

в ПП / РПД Б1.В.ДВ.9.2_Информациионная безопасность

код, название ПП, РПД

Сведения об утверждении:

утвержден (а) Ученым советом факультета
(протокол Ученого совета факультета № 6 от 15.02.2018)
на 2017 год набора
Одобрен (а) на заседании методической комиссии
протокол методической комиссии факультета № 6 от 15.02.2018)
Одобрен (а) на заседании обеспечивающей кафедры ТиМПИ
протокол № 5 от 19.01.2018) Можаров М.С. (Ф. И.О. зав. кафедрой) / _____ (подпись)

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения основной образовательной программы 44.03.05 «Педагогическое образование» по профилю "Технология и Информатика"....4
2. Место дисциплины в структуре ОПОП бакалавриата....4
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....5
3.1. Объём дисциплины (модуля) по видам учебных занятий (в часах)....5
4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий....5
4.1. Разделы дисциплины (модуля) и трудоемкость по видам учебных занятий (в академических часах)....5
4.2 Содержание дисциплины (модуля), структурированное по темам (разделам)....6
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)....9
6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)....9
6.1. Паспорт фонда оценочных средств по дисциплине (модулю)....9
6.2. Типовые контрольные задания или иные материалы....10
6.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций....14
7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)....15
а) основная учебная литература:....15
б) дополнительная учебная литература:....15
8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)....15
9. Методические указания для обучающихся по освоению дисциплины (модуля)....16
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)....17
11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)....17
12. Иные сведения и (или) материалы....17
12.1. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья....17

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения основной образовательной программы 44.03.05 «Педагогическое образование» по профилю "Математика и Информатика"

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

Коды компетенции	**Результаты освоения ОПОП** ***Содержание компетенций***	**Перечень планируемых результатов обучения по дисциплине**
СПК-3	способность проектировать и развивать электронную образовательную среду, создавать, формировать, администрировать и осуществлять экспертизу качества электронных образовательных ресурсов и программно-технологического обеспечения функционирования электронной образовательной среды	**Знать:** • основные типы технических средств информатизации образования и области их применения в традиционном и мобильном обучении; • нормативно-правовую документацию, регулирующую использование компьютерной техники и программных средств в образовательном процессе; **Уметь:** • выявлять информационные потребности участников образовательного процесса и отбирать в соответствии с ними подлежащие внедрению компоненты системы управления образованием; • моделировать и проектировать структуру онлайн-курсов, онлайн-тестов, обучающих игр с учетом требований международных стандартов; **Владеть:** • технологией проектирования и реализации основных компонентов методической системы обучения информатике в электронной образовательной среде, а также технологией проектирования, реализации и оценивания образовательного процесса с использованием новейших технологий информатизации образования; • способами анализа и отбора методов и средств обеспечения информационной безопасности при работе в электронной среде обучения
ПК-12	способностью руководить учебно-исследовательской деятельностью обучающихся	**Знать:** • технологии организации учебно-исследовательской деятельности обучающихся. **Уметь:** • оказывать содействие в подготовке обучающихся к участию в предметных олимпиадах, конкурсах, исследовательских проектах, интеллектуальных марафонах, турнирах и ученических конференциях. **Владеть:** • навыками организации учебно-исследовательской деятельности обучающихся, школьных научных сообществ.

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина «Информационная безопасность» относится к вариативной части базового цикла дисциплин (Б1.В.ДВ.9).

Для освоения дисциплины «Информационная безопасность» студенты используют знания, умения, навыки, сформированные в процессе изучения студентами информационно-технологических дисциплин, а также практический опыт работы с вычислительной техникой.

Для освоения данной дисциплины необходимы компетенции, сформированные в процессе изучения дисциплин «Архитектура компьютера», «Программное обеспечение», «Компьютерные сети и интернет-технологии», «Операционные системы».

Дисциплина (модуль) изучается на __3 курсе в __6__ 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 __2__ зачетных единиц (ЗЕТ), ___72_____ академических часа.

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

Объём дисциплины	**Всего часов** *для очной формы обучения*
Общая трудоемкость дисциплины	72
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	36
Аудиторная работа (всего):	36
в т. числе:	
Лекции	12
Семинары, практические занятия	
Практикумы	
Лабораторные работы	24
в т.ч. в активной и интерактивной формах	10
Внеаудиторная работа (всего):	36
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
Вид промежуточной аттестации обучающегося (зачет)	зачет

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 в области информационной безопасности, управления и	6	2		4	УО, лаборатор-ная 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		самостоя-тельная работа обучаю-щихся	
		всего	лекции	семинары, практи-ческие занятия		
	администрирования в образовании.					
2.	Международные стандарты и нормативно-правовое обеспечение информационной безопасности.	6	2		4	УО, ПР-4, лаборатор-ная работа
3.	Политика информационной безопасности	12	2	6	4	ИЗ, лаборатор-ная работа
4.	Основные типы технических средств обеспечения информационной безопасности и области их применения в традиционном и мобильном обучении.	15	1	8	6	ИЗ, лаборатор-ная работа
5.	Анализ угроз информационной безопасности	11	1	4	6	УО, лаборатор-ная работа (проект)
6.	Специфика реализации технологий информационной безопасности.	12	2	4	6	УО, лаборатор-ная работа
7.	Требования информационной безопасности к защищаемым системам.	10	2	2	6	ПР-1, лаборатор-ная работа
8.	ИТОГО	72	12	24	36	

Примечание:
УО - устный опрос, УО-1 - собеседование, УО-2 - коллоквиум, УО-3 - зачет, УО-4 – экзамен
ПР - письменная работа, ПР-1 - тест, ПР-2 - контрольная работа, ПР-3 эссе, ПР-4 - реферат, ПР-5 - курсовая работа, ПР-6 - научно-учебный отчет по практике, ПР-7 - отчет по НИРС,
ИЗ – индивидуальное задание;
ТС - контроль с применением технических средств, ТС-1 - компьютерное тестирование, ТС-2 - учебные задачи, ТС-3 - комплексные ситуационные задачи

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

№ п/п	Наименование раздела дисциплины	Содержание

№ п/п	Наименование раздела дисциплины	Содержание
1	**Основные понятия в области информационной безопасности, управления и администрирования в образовании**	
Содержание лекционного курса		
1.1	Основные понятия в области информационной безопасности, управления и администрирования в образовании.	Основные понятия защиты информации и информационной безопасности (ИБ) систем. Информационная безопасность, как состояние защищенности информации. Свойства информации: конфиденциальность, доступность, целостность. Обеспечение информационной безопасности.
Темы семинарских/лабораторных занятий		
1.2	Свойства информации: конфиденциальность, доступность, целостность.	Свойства информации: конфиденциальность, доступность, целостность. Примеры.
1.3	Обеспечение информационной безопасности.	Сравнительный анализ примеров обеспечения информационной безопасности.
2	**Международные стандарты и нормативно-правовое обеспечение информационной безопасности.**	
Содержание лекционного курса		
2.1	Международные стандарты и нормативно-правовое обеспечение информационной безопасности.	Международные стандарты и нормативно-правовое обеспечение информационной безопасности. Нормативно-правовая документация, регулирующая использование компьютерной техники и программных средств для обеспечения информационной безопасности.
Темы семинарских/лабораторных занятий		
2.2	Международные стандарты по информационной безопасности	Анализ и основные характеристики международных стандартов по информационной безопасности
2.3	Нормативно-правовая документация, регулирующая использование компьютерной техники и программных средств для обеспечения информационной безопасности.	Анализ нормативно-правовой документации РФ, регулирующей использование компьютерной техники и программных средств для обеспечения информационной безопасности.
3	**Политика информационной безопасности**	
Содержание лекционного курса		
3.1	Политика информационной безопасности	Политика безопасности. Распределение ролей и обязанностей. Уровни политики безопасности.
Темы семинарских/лабораторных занятий		
3.2	Уровни политики безопасности. Распределение ролей и обязанностей	Анализ уровней политики безопасности. Распределение ролей и обязанностей при организации политики безопасности в образовательных учреждениях
3.3	Политика безопасности.	Разработка и реализация политики безопасности в образовательных учреждениях
4	**Основные типы технических средств обеспечения информационной безопасности и области их применения в традиционном и мобильном обучении**	
Содержание лекционного курса		
4.1	Основные типы технических средств обеспечения информационной безопасности и области их применения в традиционном и мобильном обучении.	Основные типы технических средств обеспечения информационной безопасности и области их применения в традиционном и мобильном обучении.

№ п/п	Наименование раздела дисциплины	Содержание
Темы семинарских/лабораторных занятий		
4.2	Анализ и отбор технических средств обеспечения информационной безопасности и области их применения в традиционном и мобильном обучении	Анализ и отбор технических средств обеспечения информационной безопасности и области их применения в традиционном и мобильном обучении
4.3	Анализ и отбор средств обеспечения информационной безопасности	Анализ и отбор средств обеспечения информационной безопасности.
5	**Анализ угроз информационной безопасности**	
Содержание лекционного курса		
5.1	Анализ угроз информационной безопасности (ИБ)	Анализ угроз информационной безопасности. Классификация видов угроз ИБ. Виды угроз ИБ. Примеры реализации угроз ИБ.
Темы семинарских/лабораторных занятий		
5.2	Анализ угроз информационной безопасности	Сравнительный анализ угроз информационной безопасности
5.3	Протоколы безопасности	Использование протоколов для повышения информационной безопасности и уменьшения возможности возникновения угрозы.
6	**Специфика реализации технологий информационной безопасности**	
Содержание лекционного курса		
6.1	Специфика реализации технологий информационной безопасности	Применение защищенных виртуальных сетей. Применение межсетевых экранов. Управление доступом на уровне пользователей. Аутентификация пользователей. Технология обнаружения вторжений.
Темы семинарских/лабораторных занятий		
6.2	Применение защищенных виртуальных сетей. Применение межсетевых экранов.	Применение защищенных виртуальных сетей. Применение межсетевых экранов.
6.3	Управление доступом на уровне пользователей. Аутентификация пользователей.	Управление доступом на уровне пользователей. Аутентификация пользователей.
7	**Требования информационной безопасности к защищаемым системам**	
Содержание лекционного курса		
7.1	Требования информационной безопасности к защищаемым системам	Требования информационной безопасности к защищаемым системам. Защита информации на файловом уровне. Защита от вирусов. Централизованное управление средствами безопасности. Поддержка инфраструктуры управления открытыми ключами PKI.
Темы семинарских/лабораторных занятий		
7.2	Защита информации на файловом уровне. Защита от вирусов.	Защита информации на файловом уровне. Защита от вирусов.
7.3	Централизованное управление средствами безопасности. Поддержка инфраструктуры управления открытыми ключами PKI.	Централизованное управление средствами безопасности. Поддержка инфраструктуры управления открытыми ключами PKI.

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

Самостоятельная работа обучающихся проходит с использованием компьютера с установленным программным обеспечением. Программное обеспечение может формироваться, как из коммерческих программных средств, так и из аналогов – свободно распространяемого программного обеспечения, имеющих схожий интерфейс и возможности.

Самостоятельная работа обучающихся при изучении курса «Информационная безопасность» включает следующие виды работ:

- поиск и изучение информации по заданной теме;
- подготовка к лабораторным занятиям;
- выполнение индивидуальных заданий;
- написание рефератов на заданную тему.

Темы для рефератов:

1. Основные принципы обеспечения информационной безопасности в автоматизированных системах.
2. Причины, виды и каналы утечки информации.
3. Основные положения теории информационной безопасности информационных систем.
4. Функции монитора безопасности.
5. Управление доступом к данным.
6. Нарушения информационной безопасности вычислительных систем и причины, обуславливающие их существование.
7. Токены, смарт-карты, их применение.
8. Использование биометрических данных при аутентификации пользователей.
9. Сервисы управления доступом.
10. Механизмы доступа данных в операционных системах, системах управления базами данных.
11. Ролевая модель управления доступом.
12. Протоколирование и аудит. Задачи и функции аудита.
13. Активный аудит, методы активного аудита.
14. Защита Интернет-подключений, функции и назначение межсетевых экранов.
15. Виртуальные частные сети (VPN).
16. Защита данных и сервисов от воздействия вредоносных программ.
17. Вредоносное ПО. Антивирусное программное обеспечение.
18. Защита электронной почты. Спам, борьба со спамом.

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.	Основные понятия в области информационной безопасности, управления и администрирования в образовании.	СПК-3, ПК-12	Устный опрос
2.	Международные стандарты и нормативно-правовое обеспечение информационной безопасности.	СПК-3, ПК-12	Устный опрос
3.	Политика информационной безопасности	СПК-3, ПК-12	Индивидуальное

№ п/п	Контролируемые разделы (темы) дисциплины (результаты по разделам)	Код контролируемой компетенции* (или её части)	наименование оценочного средства
			задание для выполнения на компьютере
4.	Основные типы технических средств обеспечения информационной безопасности и области их применения в традиционном и мобильном обучении.	СПК-3, ПК-12	Индивидуальное задание для выполнения на компьютере
5.	Анализ угроз информационной безопасности	СПК-3, ПК-12	Контрольные вопросы, лабораторная работа
6.	Специфика реализации технологий информационной безопасности.	СПК-3, ПК-12	Контрольные вопросы, тестирование, лабораторная работа
7.	Требования информационной безопасности к защищаемым системам.	СПК-3, ПК-12	Контрольные вопросы, тестирование, лабораторная работа

6.2. Типовые контрольные задания или иные материалы

6.2.1. Зачет

а) Тест:

1. 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

2. 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

3. 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

4. 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)

5. 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
6. 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. Физические методы защиты информации относятся к
a. организационно-правовым методам
b. инженерно-техническим методам
c. аппаратным методам
d. программным методам
8. В какой статье Уголовного кодекса РФ предусматривается наказание за создание, использование и распространение вирусов?
a. 272
b. 273
c. 274
9. Какой открытый стандартный многосторонний протокол предназначен для проведения платежей в Интернете с использованием пластиковых карточек:
a. SET
b. GSS-API
c. IPSec
d. TLS
e. SSL
10. Угрозой информационной безопасности называют
a. попытка реализации события, действия, процесса или явления, которая может привести к нанесению ущерба чьим-либо интересам
b. средства, используемые злоумышленниками для установки средств удаленного управления компьютером
c. совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации
d. промежуток времени от момента, когда появляется возможность использовать уязвимость в защите, и до момента, когда она ликвидируется
11. Политика какого уровня определяет решение вопросов, касающихся отдельных аспектов информационной безопасности, но важных для различных систем, эксплуатируемых организацией:
a. верхнего
b. среднего
c. нижнего
12. Предоставление полномочий на выполнение определенных действий в некоторой информационной системе называется...
a. аутентификацией
b. мандатным контролем доступа
c. авторизацией
d. инагурацией
e. идентификацией
13. Как называется угроза, когда создаются препятствия для использования ресурсов информационных систем легальными пользователями:
a. угроза нарушения конфиденциальности
b. угроза нарушения целостности
c. угроза отказа служб
d. угроза раскрытия параметров системы

14. К оценочным стандартам относят:

a. ISO/IEC 15408 "Критерии оценки безопасности информационных технологий"

b. Руководящие документы Гостехкомиссии России

c. Британский стандарт BS 7799 "Управление информационной безопасностью. Практические

d. X.800 "Архитектура безопасности для взаимодействия открытых систем"

e. Федеральный стандарт США "Требования безопасности для криптографических модулей" правила"

15. Физические методы защиты информации относятся к

a. инженерно-техническим методам
b. организационно-правовым методам
c. аппаратным методам
d. программным методам

16. Как называется метод изменения кодов программ и данных с целью сделать их непонятными для не посвященных?

a. дополнение данных
b. криптография
c. ключи кодирования
d. хеширование
e. верификация
f. экранирование

17. Что не относится к функциям защиты информации от копирования?

a. идентификация среды, из которой будет запускаться программа
b. аутентификация среды, из которой запущена программа
c. реакция на запуск из несанкционированной среды
d. идентификация субъектов и объектов
e. противодействие изучению алгоритмов работы системы

18. В каком году был утвержден проект закона «О коммерческой тайне»?

a. 1993
b. 1995
c. 1999
d. 2006

19. Процедура проведения анализа с целью определить подлинность имени объекта называется …

a. аутентификация
b. экранирование
c. верификация
d. идентификация

20. Самым надежным методом защиты от вирусов является использование …

a. антивирусной программы
b. защитного экрана
c. специальных контроллеров и их ПО

б) критерии оценивания компетенций (результатов):

Итоговый контроль по дисциплине проводится в форме зачета с оценкой в 10 семестре.

Для получения зачета с оценкой, обучающиеся должны выполнить текущие требования к формированию компетенции по дисциплине.

Учитываются устные опросы, проводимые во время практических занятий, и итоговый тест. Оценивается выполнение индивидуальных заданий за компьютером в ходе лабораторных работ.

Критерии оценки сформированности компетенций в процессе устного опроса (качества устного ответа обучающегося):

– умение анализировать научно-методическую и учебную литературу;

– умение обобщать материал и делать выводы;

– знание основных понятий курса,
– знание основных этапов применения информационных технологий.

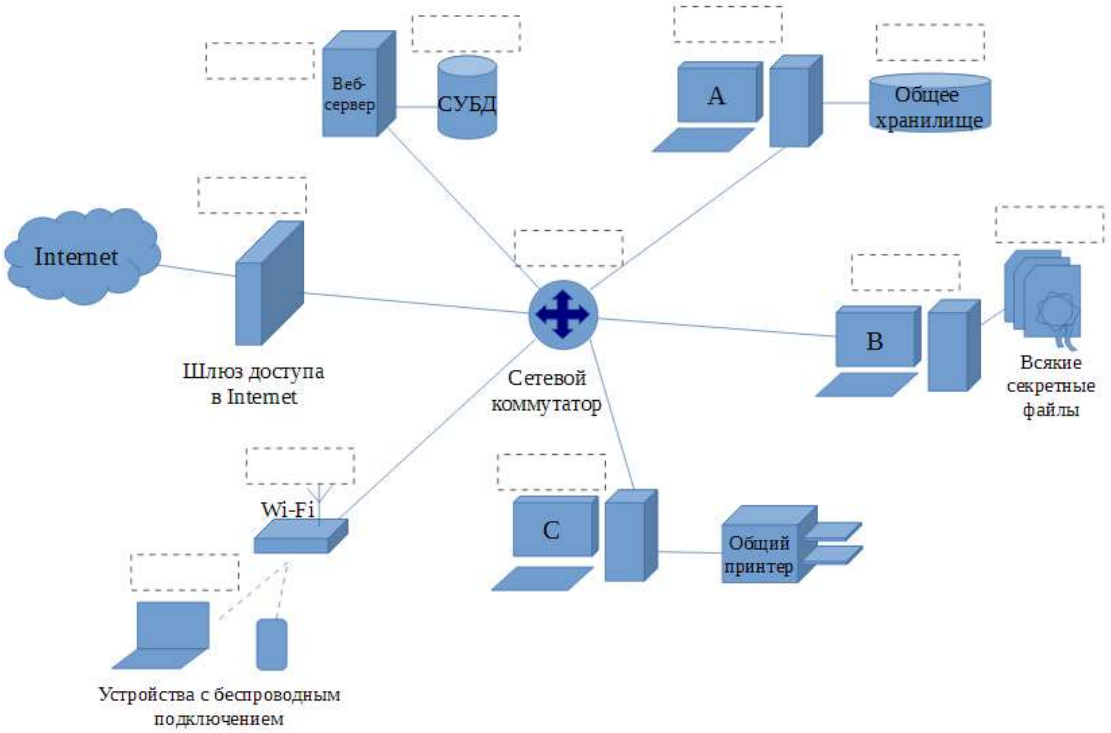
в) описание шкалы оценивания:
Тест состоит из 20 вопросов – общее количество баллов 20. За каждый правильный ответ – 1 балл.

6.2.2. Наименование оценочного средства (*в соответствии с таблицей п. 6.1***)**

а) типовые задания (вопросы) – образец:

ФИО, группа _____

Задание 1. Предложите достаточные защитные механизмы на изображенной схеме офисной ЛВС. Впишите номера (один или несколько) из списка ниже в поля рядом с компонентами системы. Известно, что ПЭВМ A, B, C используются, в том числе, для работы в Интернете и с электронной почтой.



1 – Антивирус; 2 – Межсетевое экранирование; 3 – Шифрование; 4 – Средства ЭЦП; 5 – Управление удаленным доступом; 6 – Проверка целостности; 7 – Управление маршрутизацией; 8 – Протоколирование; 9 – Резервирование электропитания; 10 – Управление локальным доступом.

Какие угрозы будут наиболее вероятными в рассматриваемой выше системе?

_____

Какие изменения структуры системы вы можете предложить для повышения ее защищенности?

_____

Задание 2. Какие три угрозы ИБ вы могли бы указать в качестве наиболее вероятных, с которыми в настоящее время может столкнуться любой человек, независимо от рода его занятий? Дайте краткий анализ по схеме «источник угрозы – способ реализации – потенциальный ущерб – защитные меры».

1) _____

2) _____
3) _____

б) критерии оценивания компетенций (результатов):

Результаты зачета определяются оценками «отлично», «хорошо», «удовлетворительно», «не удовлетворительно». При выставлении оценок учитывается уровень приобретенных компетенций обучающегося по составляющим «знать», «уметь», «владеть». Компонент «знать» оценивается теоретическими вопросами по содержанию дисциплины, компоненты «уметь» и «владеть» – практическими заданиями. Важное значение имеют объем, глубина знаний, аргументированность и доказательность ответов обучающегося, а также его общий кругозор.

в) описание шкалы оценивания:

При выставлении оценки экзаменатор руководствуется следующим:

- обучающийся знает нормативно-правовую документацию, регулирующую использование компьютерной техники и программных средств в образовательном процессе; основные типы, структуру и характеристики образовательных объектов; специфику реализации технологий проблемного, проектного и исследовательского обучения в электронной информационно-образовательной среде;
- обучающийся умет выявлять информационные потребности участников образовательного процесса и отбирать в соответствии с ними подлежащие внедрению компоненты системы управления образованием; оценивать функциональные возможности систем управления образовательным контентом с позиций реализации современных методик и технологий; моделировать и проектировать структуру онлайн-курсов, онлайн-тестов, обучающих игр с учетом требований международных стандартов;
- обучающийся владеет способами анализа и отбора методов и средств обеспечения информационной безопасности при работе в электронной среде обучения.

Оценивается ответ, если обучающимся допущены незначительные неточности, которые он исправляет путем наводящих вопросов со стороны преподавателя.

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

Промежуточная аттестация по дисциплине (зачет) включает следующие формы контроля в системе БРС:

Вид деятельности	Общее количество, пара	Максимальный балл
Лекция	6	6
Лабораторная работа	12	48
Реферат	1	3
Индивидуальная работа	2	20
Устный опрос	2	8
Зачет (итоговый тест)	1	15
Максимальное количество набранных баллов:		100

Итоговый балл получается простым сложениям набранных баллов по формам контроля.

Устный опрос – максимальное – 4 балла, пороговое значение – 2 балла.

Индивидуальная работа состоит из двух заданий – максимальное 10 баллов за одно задание, пороговое – 6 баллов за задание.

Итоговый тест – максимальное – 20 баллов, пороговое – 10 баллов.

За посещение занятий: лекция – 1 балл, лабораторное занятие – 0.5 балла.

При выполнении лабораторных заданий на занятие на 51–65 % – 1 балл, на 66–85 % – 2 балла, на 86 –100 % – 3 балла.

Для оценки необходимо набрать более 50 баллов, а также преодолеть пороговые значения по всем видам контроля:

- оценка «отлично» ставится, если студент набрал 86–100 баллов;
- оценка «хорошо» – 66–85 баллов;
- оценка «удовлетворительно» – 51–65 баллов;
- оценка «не удовлетворительно» – 0–50 баллов.

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

а) основная учебная литература:

1. Защита информации [Электронный ресурс] : учебное пособие / А. П. Жук [и др.]. - 2-е изд. – Электрон. текстов. данные. - Москва : РИОР : ИНФРА-М, 2015. - 392 с. - (Высшее образование: Бакалавриат; Магистратура). - Режим доступа: http://znanium.com/bookread2.php?book=474838

2. Шаньгин, В. Ф. Информационная безопасность [Электронный ресурс] : учебное пособие / В. Ф. Шаньгин. — Электрон. дан. — Москва : ДМК Пресс, 2014. — 702 с. — Режим доступа: http://e.lanbook.com/book/50578.

б) дополнительная учебная литература:

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

2. Спицын, В. Г. Информационная безопасность вычислительной техники [Электронный ресурс] : учебное пособие / В. Г. Спицын ; Министерство образования и науки РФ ; Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). – Электрон. текстов. данные. - Томск : Эль Контент, 2011. - 148 с. : ил.,табл., схем. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=208694

3. Сычев, Ю.Н. Основы информационной безопасности [Электронный ресурс] : учебно-практическое пособие / Ю. Н. Сычев. – Электрон. текстов. данные. - Москва : Евразийский открытый институт, 2010. - 328 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=90790

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

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

Электронно-библиотечная система «Знаниум» - www.znanium.com – Договор № 44/2017 от 21.02.2017 г., срок до 15.03.2020 г.

Доступ из локальной сети НФИ КемГУ свободный, неограниченный, с домашних ПК – авторизованный. Кол-во возможных подключений – **4000.**

Электронно-библиотечная система «Университетская библиотека онлайн» http://biblioclub.ru/ – базовая часть, контракт № 031 - 01/17 от 02.02.2017 г., срок до 14.02.2018 г., неограниченный доступ для всех зарегистрированных пользователей КемГУ.

Доступ из локальной сети НФИ КемГУ свободный, неограниченный, с домашних ПК – авторизованный. Кол-во возможных подключений – **7000.**

Электронно-библиотечная система «Юрайт» - www.biblio-online.ru. Доступ ко всем произведениям, входящим в состав ЭБС. Договор № 30/2017 от 07.02.2017 г., срок до 16.02.2018г.

Доступ из локальной сети НФИ КемГУ свободный, с домашних ПК – авторизованный. Кол-во одновременных доступов - **безлимит .**

Электронная полнотекстовая **база данных периодических изданий по общественным и гуманитарным наукам** ООО «ИВИС», https://dlib.eastview.com, договор № 196-П от 10.10.2016 г., срок действия с 01.01.2017 по 31.12.2017 г., доступ предоставляется из локальной сети НФИ КемГУ.

Межвузовская электронная библиотека (МЭБ) - https://icdlib.nspu.ru/ - сводный информационный ресурс электронных документов для образовательной и научно-исследовательской деятельности педагогических вузов. НФИ КемГУ является участником и пользователем МЭБ. Договор о присоединении к МЭБ от 15.10.2013 г,, доп. соглашение от 01.04.2014 г. Доступ предоставляется из локальной сети НФИ КемГУ.

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)

Лекции читаются с использованием слайд-презентаций, видео и аудио-материалов.

В процессе текущего контроля используется интерент-тестирование. Взаимодействие с обучающимися организуется с помощью электронной почты, форумов, кафедрального сайта, скайпа. Обучающиеся привлекаются к участию в видеоконференциях, вебинарах.

Используются 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

Для слабовидящих и слепых обучающихся:

– предоставляются учебно-методические материалы шрифтом Times New Roman 26;

– создаются условия для использования собственных увеличивающих устройств, специальных технических средств, диктофонов;

– в работе с маломобильными обучающимися предусматривается возможность консультаций посредством электронной почты и программы Skype;

– все письменные задания для данной категории обучающихся озвучиваются.

Для глухих и слабослышащих обучающихся:

– разрешается пользоваться специальными техническими средствами (звукоусиливающей аппаратурой);

– используется разнообразный наглядный материал (схемы, таблицы, мультимедийные презентации);

– в работе с маломобильными обучающимися предусматривается возможность консультаций посредством электронной почты и программы Skype;

– все устные задания предоставляются в письменном виде.

Обучающимся с нарушениями функций опорно-двигательного аппарата:

– предоставляются мультимедийные материалы по изучаемым дисциплинам;

– разрешается использование собственных компьютерных средств;

– в работе с маломобильными обучающимися предусматривается возможность консультаций посредством электронной почты и программы Skype.

Составитель (и): Валеева Ю.И., старший преподаватель, Дробахина А.Н., доцент

(*фамилия, инициалы и должность преподавателя (ей)*)

Макет рабочей программы дисциплины (модуля) одобрен научно-методическим советом (протокол № 8 от 09.04.2017 г.)