Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кемеровский государственный университет»
Кузбасский гуманитарно-педагогический институт
федерального государственного бюджетного образовательного учреждения высшего образования
«Кемеровский государственный университет»

Факультет информатики, математики и экономики

«УТВЕРЖДАЮ»
Декан ФИМЭ
_А.В. Фомина
«10» февраля 2022 г.

Рабочая программа дисциплины

__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, заочная_____
Очная, очно-заочная, заочная

Год набора 2018

Новокузнецк 2022

СОДЕРЖАНИЕ

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 основной профессиональной образовательной программы бакалавриата и изучения данной дисциплины обучающийся должен освоить Компетенции:

специальная профессиональная компетенция СПК-1;

профессиональная компетенция ПК-12.

Перечень планируемых результатов обучения по дисциплине в таблице 1.

Таблица 1 – Результаты обучения по дисциплине

Коды компетенции	**Результаты освоения ОПОП** ***Содержание компетенций***	**Перечень планируемых результатов обучения по дисциплине**
СПК-1	способен осуществлять разработку и реализацию образовательных программ основного и среднего общего образования по информатике на основе специальных научных знаний в предметной области “Информатика”	**Знать:** • основные математические методы получения, хранения, обработки, передачи и использования информации; • регламенты обеспечения информационной безопасности, методы и средства защиты информации, типовые уязвимости, учитываемые при эксплуатации устанавливаемого программного обеспечения; **Уметь**: • применять математический аппарат анализа и синтеза информационных систем; • настраивать программное обеспечение в соответствии с регламентами обеспечения информационной безопасности, использовать программно-аппаратные и программные средства защиты информации; **Владеть** • современными формализованными математическими, информационно-

		логическими и логико-семантическими моделями и методами представления, сбора и обработки информации; • 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 (модуль) изучается на 3 курсе в 6 семестре.

Данная дисциплина относится к обязательным дисциплинам вариативной части профессионального цикла ООП бакалавриата.

Структурно-логическая схема формирования в ОПОП компетенций, закрепленных за дисциплиной

Таблица 2 – Порядок формирования компетенции СПК-1

Предшествующие дисциплины, практики	Последующие дисциплины, практики
Б1.Б.15.02 Методика обучения предметам (информатика) Б1.В.07 Математическая логика Б1.В.12 Теория алгоритмов Б1.В.17 Теоретические основы информатики Б1.В.18 Компьютерное	Б1.В.ДВ.16.01 Информатизация управления образовательным процессом Б1.В.ДВ.16.02 Управление образованием на основе информационно-коммуникационных технологий Б2.В.02(П) Производственная практика. Практика по получению

моделирование Б1.В.20 Практикум по решению задач на компьютере Б1.В.21 Основы искусственного интеллекта Б1.В.23 Операционные системы, сети и интернет-технологии Б1.В.ДВ.03.01Программирование на JavaScript Б1.В.ДВ.03.02 Видеомонтаж Б1.В.ДВ.07.01 Компьютерная графика Б1.В.ДВ.07.02 Компьютерный дизайн Б1.В.ДВ.10.01 Программное обеспечение Б1.В.ДВ.10.02 Новые информационные технологии Б1.В.ДВ.12.01Программирование Б1.В.ДВ.12.02Алгоритмические языки программирования	профессиональных умений и опыта профессиональной деятельности Б2.В.03(П) Производственная практика. Педагогическая практика Б2.В.04(П) Производственная практика. Научно-исследовательская работа Б2.В.05(Пд)Производственная практика. Преддипломная практика Б1.В.ДВ.14.01 Информационные системы Б1.В.ДВ.14.02 Системы управления базами данных Б1.В.ДВ.15.01 Архитектура компьютера Б1.В.ДВ.15.02 Вычислительная техника

Таблица 3 – Порядок формирования компетенции ПК-12

Предшествующие дисциплины, практики	Последующие дисциплины, практики
Б1.Б.02 Психолого-педагогические основания профессиональной деятельности Б1.Б.02.05 Информационно-коммуникационные технологии в образовании	Б1.В.01 Технологии и методы проектирования и реализации программ основного общего образования Б1.В.01.05 Организация исследовательской и проектной деятельности обучающегося по математике Б1.В.01.06 Организация исследовательской и проектной деятельности обучающегося по информатике Б2.В.04(П) Производственная практика. Научно-исследовательская работа Б2.В.05(Пд)Производственная практика. Преддипломная практика

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.

Курсовая работа не планируется.

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

Объём дисциплины	**Всего часов**	
	для очной формы обучения	*для заочной формы обучения*
Общая трудоемкость дисциплины	72	72
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	36	12
Аудиторная работа (всего):	36	12
в т. числе:		
Лекции	12	4
Семинары, практические занятия		
Практикумы		
Лабораторные работы	24	8
в т.ч. в активной и интерактивной формах		
Внеаудиторная работа (всего):	36	56
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	56
Вид промежуточной аттестации обучающегося (зачет)	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 администрирования в образовании.	6	2		4	УО, лаборатор-ная работа
2.	Международные стандарты	6	2		4	УО, ПР-4,

№ 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		
	и нормативно-правовое обеспечение информационной безопасности.					лабораторная работа
3.	Политика информационной безопасности	12	2	6	4	ИЗ, лабораторная работа
4.	Основные типы технических средств обеспечения информационной безопасности и области их применения в традиционном и мобильном обучении.	15	1	8	6	ИЗ, лабораторная работа
5.	Анализ угроз информационной безопасности	11	1	4	6	УО, лабораторная работа (проект)
6.	Специфика реализации технологий информационной безопасности.	12	2	4	6	УО, лабораторная работа
7.	Требования информационной безопасности к защищаемым системам.	10	2	2	6	ПР-1, лабораторная работа
8.	ИТОГО	72	12	24	36	

для 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 в области информационной безопасности, управления и	10	1	1	8	УО, 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		самостоя-тельная работа обучаю-щихся	
		всего	лекции	семинары, практи-ческие занятия		
	администрирования в образовании.					
2.	Международные стандарты и нормативно-правовое обеспечение информационной безопасности.	10	1	1	8	УО, ПР-4, лабораторная работа
3.	Политика информационной безопасности	10	1	1	8	ИЗ, лабораторная работа
4.	Основные типы технических средств обеспечения информационной безопасности и области их применения в традиционном и мобильном обучении.	9		1	8	ИЗ, лабораторная работа
5.	Анализ угроз информационной безопасности	11	1	2	8	УО, лабораторная работа (проект)
6.	Специфика реализации технологий информационной безопасности.	9		1	8	УО, лабораторная работа
7.	Требования информационной безопасности к защищаемым системам.	9		1	8	ПР-1, лабораторная работа
8.	Зачет	4				
9.	ИТОГО	72	4	8	56	

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
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)

Методические указания по самостоятельной работе студентов опубликованы по адресу: *https://skado.dissw.ru/table/*

Самостоятельная работа обучающихся при изучении курса «Методы и средства защиты информации» включает следующие виды работ:

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

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

Форма промежуточной аттестации – зачет.

6.1. Типовые контрольные задания или иные материалы

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

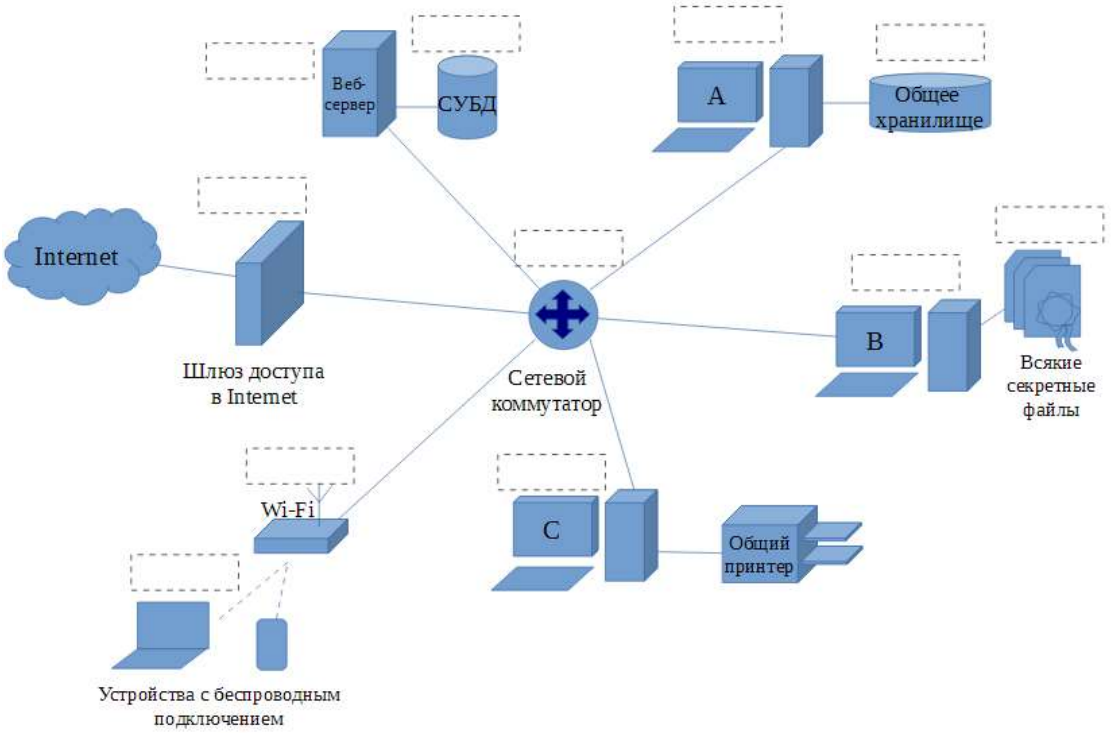
20. Самым надежным методом защиты от вирусов является использование …

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

типовые задания (задачи):

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) _____

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

Для положительной оценки по результатам освоения дисциплины обучающемуся необходимо выполнить все установленные виды учебной работы. Оценка результатов работы обучающегося в баллах (по видам) приведена в таблице.

Таблица 6 - Балльно-рейтинговая оценка результатов учебной работы обучающихся по видам (БРС)

Учебная работа (виды)	Сумма баллов	Виды и результаты учебной работы	Оценка в аттестации	Баллы
Текущая учебная работа в семестре (Посещение занятий по расписанию и выполнение заданий)	**80**	Лекционные занятия (конспект) (6 занятий)	2 балла посещение 1 лекционного занятия	6- 12
		Лабораторные работы (отчет о выполнении лабораторной работы) (12 работ).	3 балла - посещение 1 практического занятия и выполнение работы на 51-65% 4 баллов посещение 1 занятия и существенный вклад на занятии в работу всей группы, самостоятельность и выполнение работы на 65,1-85% 5 баллов – посещение 1 занятия и существенный вклад на занятии в работу всей группы, самостоятельность и выполнение работы на 85,1-100%	30- 60
		Реферат	4 баллов (пороговое значение) 8 баллов (максимальное значение)	4 - 8
Итого по текущей работе в семестре				40-80
Промежуточная аттестация (экзамен)	20	Тест.	11 баллов (пороговое значение) 20 баллов (максимальное значение)	11 - 20
Итого по промежуточной аттестации				11 - 20
Суммарная оценка по дисциплине/ Сумма баллов текущей и промежуточной аттестации				51 – 100 б.

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», современных профессиональных баз данных (СПБД) и информационных справочных систем (ИСС) необходимых для освоения дисциплины

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

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

Современные профессиональные базы данных (СПБД) и информационные справочные системы (ИСС) по дисциплине

Science Direct содержит более 1500 журналов издательства Elsevier, среди них издания по экономике и эконометрике, бизнесу и финансам, социальным наукам и психологии, математике и информатике.

Информационная система «Единое окно доступа к образовательным ресурсам. Раздел. Информатика и информационные технологии» -

http://www.window.edu.ru .

Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки- https://github.com/

База книг и публикаций Электронной библиотеки "Наука и Техника" - http://www.n-t.ru

9. Методические указания для обучающихся по освоению дисциплины

Образовательная программа и методические указания размещены на сайте НФИ КемГУ https://eios.nbikemsu.ru/

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

Материально-техническая база

Учебные занятия по дисциплине проводятся в учебных аудиториях НФИ КемГУ:

Информационная безопасность	508 Компьютерный класс Учебная аудитория для проведения занятий лекционного типа, занятий лабораторного типа, для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации Специализированная (учебная) мебель: доска меловая, кафедра, столы, стулья Оборудование для презентации учебного материала: компьютер преподавателя, проектор, экран, 18 компьютеров Лабораторное оборудование: стационарное – компьютеры для обучающихся (18 шт.). Используемое программное обеспечение: MSWindows (MicrosoftImaginePremium 3 year по сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.), Яндекс.Браузер (отечественное свободно распространяемое ПО), Firefox 14 (свободно распространяемое ПО), Opera 12 (свободно распространяемое ПО),LibreOffice (свободно распространяемое ПО), FoxitReader (свободно распространяемое ПО), XAMPP (свободно распространяемое ПО), Denwer (свободно распространяемое ПО), MicrosoftVisualStudio (MicrosoftImaginePremium 3 year по сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.), Антивирусное ПО ESET Endpoint Security, лицензия №EAV-0267348511 до 30.12.2022.. Интернет с обеспечением доступа в ЭИОС	654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19

11. Иные сведения и (или) материалы

Темы 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.

Составитель (и): 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.)