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

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.09.01_Методы и средства защиты информации
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 управления и администрирования информационных систем. Источники атак на	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		
	информацию, риски.					
2.	Международные стандарты и нормативно-правовое обеспечение в электронной информационно-образовательной среде.	6	2		4	УО, ПР-4
3.	Криптографические модели, специфика реализации технологий.	12	2	6	4	ИЗ, лабораторная работа
4.	Алгоритмы шифрования.	15	1	8	6	ИЗ, лабораторная работа
5.	Алгоритмы аутентификации пользователей.	11	1	4	6	УО, лабораторная работа
6.	Многоуровневая защита корпоративных сетей. Требования к системам защиты информации.	12	2	4	6	УО, лабораторная работа
7.	Анализ и отбор методов и средств обеспечения защиты информации в сетях.	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 управления и администрирования информационных систем. Источники атак на информацию, риски.	10	1	1	8	УО, ПР-4
2.	Международные стандарты и нормативно-правовое обеспечение в электронной	10	1	1	8	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		самостоя-тельная работа обучаю-щихся	
		всего	лекции	семинары, практи-ческие занятия		
	информационно-образовательной среде.					
3.	Криптографические модели, специфика реализации технологий.	10	1	1	8	ИЗ, лаборатор-ная работа
4.	Алгоритмы шифрования.	9	0	1	8	ИЗ, лаборатор-ная работа
5.	Алгоритмы аутентификации пользователей.	11	1	2	8	УО, лаборатор-ная работа
6.	Многоуровневая защита корпоративных сетей. Требования к системам защиты информации.	9	0	1	8	УО, лаборатор-ная работа
7.	Анализ и отбор методов и средств обеспечения защиты информации в сетях.	9	0	1	8	ПР-1, лаборатор-ная 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 управления и администрирования информационных систем. Источники атак на информацию, риски**	
Содержание лекционного курса		
1.1	Основные понятия в области управления и администрирования информационных систем. Источники атак на информацию, риски.	Основные понятия в области управления и администрирования информационных систем. Источники, риски и формы атак на информацию. Понятие угрозы. Необходимость защиты информационных систем и телекоммуникаций. Основные задачи обеспечения защиты

№ п/п	Наименование раздела дисциплины	Содержание
		информации.
2	**Международные стандарты и нормативно-правовое обеспечение в электронной информационно-образовательной среде**	
Содержание лекционного курса		
2.1	Международные стандарты и нормативно-правовое обеспечение в электронной информационно-образовательной среде.	Международные стандарты информационного обмена. Стандарты безопасности. Нормативно-правовая документация, регулирующая использование компьютерной техники и программных средств. Свойства информации: конфиденциальность, доступность, целостность.
3	**Криптографические модели, специфика реализации технологий**	
Содержание лекционного курса		
3.1	Криптографические модели, специфика реализации технологий.	Криптографические модели. Модели безопасности основных ОС. Особенности современных информационных систем, факторы влияющие на безопасность информационной системы. Идентификация и аутентификация. Парольные схемы аутентификации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом).
Темы семинарских/лабораторных занятий		
3.2	Криптографические методы защиты.	Реализация криптографического преобразования информации по одному из доступных алгоритмов.
3.3	Парольные схемы аутентификации. Симметричные схемы аутентификации субъекта.	Использование симметричных схем в криптографии.
3.4	Несимметричные схемы аутентификации (с открытым ключом).	Использование несимметричных схем в криптографии.
4	**Алгоритмы шифрования**	
Содержание лекционного курса		
4.1	Алгоритмы шифрования.	Алгоритмы шифрования.
Темы семинарских/лабораторных занятий		
4.2	Алгоритмы шифрования	Шифрование сообщений с помощью простейших алгоритмов.
4.3	Алгоритмы шифрования	Шифрование сообщений с помощью алгоритмов Керкхоффса, RSA.
4.4	Алгоритмы шифрования	Написание программы шифрования сообщений на языке объектно-ориентированного программирования
4.5	Алгоритмы шифрования	Расшифровка и дешифровка сообщений
5	**Алгоритмы аутентификации пользователей**	
Содержание лекционного курса		
5.1	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.
Темы семинарских/лабораторных занятий		
5.2	Алгоритмы	Изучение принципов аутентификации пользователей веб-

№ п/п	Наименование раздела дисциплины	Содержание
	аутентификации пользователей.	сервисов.
5.3	Электронная цифровая подпись	Изучение принципов формирования и использования электронной цифровой подписи.
6	**Многоуровневая защита корпоративных сетей. Требования к системам защиты информации**	
Содержание лекционного курса		
6.1	Многоуровневая защита корпоративных сетей. Требования к системам защиты информации.	Многоуровневая защита корпоративных сетей. Требования к системам защиты информации. Иерархический метод разработки защищенных систем. Структурный принцип. Основные этапы разработки защищенной системы.
Темы семинарских/лабораторных занятий		
6.2	Требования к системам защиты информации. Иерархический метод разработки защищенных систем.	Иерархический метод разработки защищенных систем.
6.3	Структурный принцип. Основные этапы разработки защищенной системы.	Структурный принцип разработки защищенных систем.
7	**Анализ и отбор методов и средств обеспечения защиты информации в сетях**	
Содержание лекционного курса		
7.1	Анализ и отбор методов и средств обеспечения защиты информации в сетях.	Защита информации в сетях. Анализ и отбор методов и средств обеспечения защиты информации в сетях. Классы защищенности компьютерных систем. Интерпретация и развитие критериев защиты информации в сетях.
Темы семинарских/лабораторных занятий		
7.2	Анализ и отбор методов и средств обеспечения защиты информации в сетях.	Определение наличия и удаление вредоносного ПО с помощью программных средств антивирусного ПО. Исследование механизмов парольной защиты, методов противодействия атакам на пароль.
7.3	Анализ и отбор методов и средств обеспечения защиты информации в сетях.	Управление правами доступа к ресурсам ОС, ИС и веб-сервисов.
7.4	Анализ и отбор методов и средств обеспечения защиты информации в сетях.	Развертывание веб-сервера. Настройка параметров безопасности. Испытания эффективности его защиты.

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

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. 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

9. 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

10. 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

11. 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

12. Монитор обращений ("ядро безопасности") должен обладать как минимум тремя важными характеристиками:
a. Документированность
b. Изолированность
c. Полнота
d. Прозрачность
e. Верифицируемость

13. 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

14. Предоставление полномочий на выполнение определенных действий в некоторой информационной системе называется...
a. аутентификацией
b. мандатным контролем доступа
c. авторизацией

d. инагурацией
e. идентификацией

15. Протокол передачи данных, обеспечивающий шифрование потока данных на транспортном уровне:

a. TCP
b. SSL
c. RDP
d. SSH
e. VPN

Практическое задание. Алгоритм RSA

Используя алгоритм RSA отправить шифрованное сообщение одному пользователю и получить и расшифровать сообщение от другого пользователя. Заполнить и сдать карточку со своими действиями:

ФИ студента _____ Группа _____

Действие	**Результат**	**Кому отправлено или от кого получено**
Придуманный открытый ключ		
Придуманный секретный ключ		–
Шифрованное сообщение		
Расшифрованное сообщение		–
Полученный открытый ключ		
Открытое сообщение		–
Шифрованное сообщение		

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	30- 60

			и существенный вклад на занятии в работу всей группы, самостоятельность и выполнение работы на 85,1-100%	
		Реферат	4 баллов (пороговое значение) 8 баллов (максимальное значение)	4 - 8
Итого по текущей работе в семестре				40-80
Промежуточная аттестация	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.Баранова, Е. К. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / Е. К. Баранова , А. В. Бабаш . - 3-е изд. – Электрон. текстов. данные. - Москва : РИОР : ИНФРА-М, 2016. - 322 с. - (Высшее образование). – Режим доступа: http://znanium.com/bookread2.php?book=495249

2. 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

б) дополнительная учебная литература:

1. 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

2. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 201 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-014976-9. - Текст : электронный. - Режим доступа: URL: https://znanium.com/catalog/product/

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:

Методы и средства защиты информации	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	654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19

	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	

11. Иные сведения и (или) материалы

Темы рефератов:

1. Классификация компьютерных преступлений. Группы компьютерных преступлений. Хакерство в мире и в России.
2. Биометрические системы идентификации
3. Анализ программ родительского контроля. Родительский контроль в составе антивирусных программ и операционных систем
4. Основные психолого-педагогические приемы и средства по обеспечению информационной безопасности детей в Интернете.
5. Системы управления доступом в Интернет и контроля корпоративной электронной почты
6. Утечки информации: источники, правовые и технологические аспекты борьбы.
7. Утилизация данных: проблемы повторного использования.
8. SELinux: реализация мандатного (принудительного) контроля доступа.
9. Распределенные системы управления доступом LDAP и ActiveDirectory: описание и сравнение.
10. Rootkits –примеры (для Windows, для *nix), методы и средства выявления и противодействия
11. Применение технологий «honeypots» для обеспечения сетевой безопасности.
12. SQL-инъекции: принципы атак, способы их обнаружения и противодействия.
13. Атаки межсайтового скриптинга (XSS-атаки): принципы атак, способы их обнаружения и противодействия. 10.Проблемы противодействия фишингу и фармингу.
14. P2P-приложения: тенденции развития и аспекты безопасности.
15. Безопасность Web-браузеров.
16. Безопасность беспроводных технологий.
17. Виртуальные частные сети (VPN) – технологии и средства организации.
18. Биометрические системы аутентификации: принципы, технологии и перспективы.
19. Средства взлома парольных систем и противодействие им.
20. Распределенные атаки отказ в обслуживании и противодействие им. «Электронное государство» - общее понятие, технологии, аспекты безопасности
21. Проблемы безопасности «виртуальных» инфраструктур e-commerce. Расследование ИТ-инцидентов
22. Эволюция вредоносного ПО (malware) и средств борьбы с ним.
23. СПАМ: способы распространения, принципы и средства противодействия
24. Методы защиты от нелегального использования ПО (и др. ITресурсов).

25. Безопасность информационных систем построенных с использованием с использованием технологий виртуализации.
26. Методы и средства борьбы и противодействия внутренним нарушителям.
27. Защита персональных данных, типовые решения.
28. Аспекты защиты информации в системах автоматизированного управления технологическими процессами.
29. Понятие политики безопасности
30. Управление рисками. Методы численного анализа рисков
31. Управление рисками. Оценка и минимизация рисков.
32. Понятие модели нарушителя. Типы моделей.
33. Методы поиска уязвимостей в информационных системах. Оценка возможности использования для проникновения.
34. Применение межсетевых экранов, цели, перечень основных уязвимостей, перечень возможных рисков.
35. Основные угрозы Интернет. Модель нарушителя.
36. Уязвимости технологии web 2.0.
37. Основы безопасной работы в интернет, минимизация рисков web 2.0.
38. Методика обеспечения бесперебойной работы информационной системы. Принципы резервирования.
39. Управление программным обеспечением, как аспект обеспечения информационной безопасности. Структура, требования, задачи.
40. Защита персональных данных. Требования, технические решения.
41. Обеспечение безопасности при облачных вычислениях.
42. Проблемы безопасности в виртуальных средах.

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.)