МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кемеровский государственный университет»
Кузбасский гуманитарно-педагогический институт

(Наименование филиала, где реализуется данная дисциплина)

Факультет информатики, математики и экономики
Кафедра информатики и общетехнических дисциплин

Утверждаю
Декан ФИМЭ
Фомина А.В.
23 июня 2021 г.

Рабочая программа дисциплины
Б1.В.ДВ.09.01 Методы и средства защиты информации

Направление подготовки
44.03.05 Педагогическое образование (с двумя профилями подготовки)

Направленность (профиль) подготовки
Технология и Информатика

Программа *академического бакалавриата*

Квалификация выпускника
бакалавр

Форма обучения
Очная

Год набора 2017

Новокузнецк 2021

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"

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**
ПК-12	способность 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.
СПК-1	Способен осуществлять разработку и реализацию образовательных программ по информатике с использованием современных информационно-коммуникационных технологий	Знать: содержание математических и информационно-технологических дисциплин, связанных с образовательной областью «Информатика». Уметь: формировать содержание обучения по информатике на основе изученных математических и информационно-технологических дисциплин; ориентироваться в современных концепциях и последних достижениях математических и информационно-технологических дисциплин, формирующих содержание обучения по информатике; использовать достижения науки для обоснования применяемых методов обучения информатике; Владеть: основными приемами работы с профессиональными базами данных и другими информационными источниками по информационно-технологическим дисциплинам для разработки и реализации образовательных программ по информатике.

2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина «Методы и средства защиты информации» относится к вариативной части базового цикла дисциплин

Для освоения дисциплины «Методы и средства защиты информации» 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.

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

Код и название компетенции	Дисциплины и практики, формирующие компетенцию ОПОП
СПК-1 Способен осуществлять разработку и реализацию образовательных программ по информатике с использованием современных информационно-коммуникационных технологий	Б1.В.02 Предметное обучение: информатика Б1.В.02.01 Компьютерное моделирование Б1.В.02.02 Теория алгоритмов Б1.В.02.03 Численные методы Б1.В.02.04 Основы искусственного интеллекта Б1.В.02.05 Операционные системы Б1.В.02.06 Компьютерные сети и интернет-технологии Б1.В.02.09 Медиаобразование Б1.В.02.10 Информационные технологии в педагогическом тестировании Б1.В.ДВ.01.01 Программирование на Java-скрипт Б1.В.ДВ.01.02 Видеомонтаж Б1.В.ДВ.02.01 3-d моделирование Б1.В.ДВ.02.02 Компьютерная графика Б1.В.ДВ.03.01 Программное обеспечение Б1.В.ДВ.03.02 Новые информационные технологии Б1.В.ДВ.04.01 Программирование Б1.В.ДВ.04.02 Языки программирования Б1.В.ДВ.05.01 Практикум по решению задач на компьютере Б1.В.ДВ.05.02 Решение задач по информатике Б1.В.ДВ.06.01 Теоретические основы информатики Б1.В.ДВ.06.02 Теория программирования Б1.В.ДВ.07.01 Информационные системы Б1.В.ДВ.07.02 Системы управления базами данных Б1.В.ДВ.08.01 Архитектура компьютера Б1.В.ДВ.08.02 Вычислительная техника Б1.В.ДВ.09.01 Методы и средства защиты информации Б1.В.ДВ.09.02 Информационная безопасность Б1.В.ДВ.13.01 Программирование в виртуальных средах Б1.В.ДВ.13.02 Разработка интерактивных презентаций Б1.В.ДВ.16.01 Компьютерные измерения и анализ массивов данных Б1.В.ДВ.16.02 Проектирование электронной образовательной среды Б1.В.ДВ.19.01 Проектирование информационных систем Б1.В.ДВ.19.02 Проектирование цифровых образовательных ресурсов Б2.В.01(У) Учебная практика. Практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности Б2.В.02(П) Производственная практика. Практика по получению профессиональных умений и опыта профессиональной деятельности Б2.В.03(П) Производственная практика. Педагогическая практика Б2.В.05(П) Производственная практика. Преддипломная практика Б3.Б.02(Д) Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты ФТД.01 Организация дистанционного образования
ПК-12 способностью руководить учебно-исследовательской деятельностью обучающихся	Б1.Б.02 Психолого-педагогические основания профессиональной деятельности Б1.Б.02.06 Технологии психолого-педагогической диагностики и педагогических измерений Б1.В.01 Технологии и методы проектирования и реализации программ основного общего образования Б1.В.01.05 Организация исследовательской и проектной

Код и название компетенции	Дисциплины и практики, формирующие компетенцию ОПОП
	деятельности обучающегося по технологии Б1.В.01.06 Организация исследовательской и проектной деятельности обучающегося по информатике Б1.В.03 Предметное обучение: технология Б1.В.03.04 Введение в теорию решения изобретательских задач Б1.В.03.06 Начертательная геометрия и черчение Б1.В.ДВ.09.01 Методы и средства защиты информации Б1.В.ДВ.09.02 Информационная безопасность Б1.В.ДВ.14.01 Программирование интеллектуальных систем Б1.В.ДВ.14.02 Программирование микроконтроллерной техники Б2.В.01(У) Учебная практика. Практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности Б2.В.04(П) Производственная практика. Научно-исследовательская работа Б2.В.05(П) Производственная практика. Преддипломная практика Б3.Б.02(Д) Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

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 с оценкой

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		самостоятельная работа обучающихся	
		всего	лекции	семинары, практические занятия		
1.	Основные понятия в области управления и администрирования информационных систем. Источники атак на информацию, риски. Основные приемы работы с профессиональными базами данных и другими информационными источниками.	6	2		4	УО, ПР-4
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	

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 информации. Основные приемы работы с профессиональными базами данных и другими информационными источниками.
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	Алгоритмы шифрования.

№ п/п	Наименование раздела дисциплины	Содержание
	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 аутентификации пользователей.	Изучение принципов аутентификации пользователей веб-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	Управление правами доступа к ресурсам ОС, ИС и веб-сервисов.

№ п/п	Наименование раздела дисциплины	Содержание
	сетях.	
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/#faculty-ed_bachelor-20

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 «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.

Темы для рефератов:

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

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

6.1. Типовые контрольные задания или иные материалы

6.1.1. Экзамен или зачет

а) Тест:

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

f. Санкционированный просмотр

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

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

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

5. Межсетевые экраны служат для
a. Изоляции некоторой сети от других с помощью настраиваемых фильтров трафика и/или анализаторов угроз
b. сбора статистики использования каналов связи сотрудниками организации
c. Для просмотра информации, распределенной по узлам нескольких сетей
d. подтверждения подлинности сообщений, принятых по сети
e. отображения информации о состоянии сети

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

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

8. 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

б) критерии оценивания компетенций (результатов):

Итоговый контроль по дисциплине проводится в форме зачета в 6 семестре.

Для получения зачета 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.

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

а) типовые задания (вопросы) – образец:

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		

Основы использования алгоритма RSA

Допустим, что **объект А** хочет передать сообщение **объекту В** в зашифрованном виде. Для этого используем алгоритм RSA. При реализации алгоритма на практике, нужно иметь возможность без сильных затрат генерировать большие простые числа, к тому же быстро решать значение ключей. Для наглядности вычисления, будем использовать небольшие числа. Но на практике используют очень большие числа (длиной 200-300 десятичных разрядов).

1. ***Объект В*** придумывает два любых больших простых числа P и Q (P≠Q).
2. ***Объект В*** решает значение модуля N = P × Q.
3. ***Объект В*** решает функцию Эйлера: **φ(N) = (P-1) × (Q-1).**
4. ***Объект В*** выбирает любым образом значение открытой экспоненты $K_в$ открытого ключа с учетом условия: $1 < K_в \leq \varphi(N)$, при этом **НОД** $(K_в, \varphi(N)) = 1$.
5. ***Объект В*** решает значение секретной экспоненты $к_с$ секретного ключа ($к_с$, N) решая алгоритм Евклида когда достигается условие: $(K_в * к_с) \bmod \varphi(N) = 1$, т.е. $к_с \equiv K_в^{-1} \bmod \varphi(N)$.
6. ***Объект В*** передает ***объекту А*** пару чисел ($K_в$, N), т.е. открытый ключ по незащищенному пути.
7. Если ***объект А*** хочет передать ***объекту В*** сообщение *M*, он должен разбить исходный открытый текст *M* на блоки, каждый из которых может быть показан в виде: $M_i = 0, 1, 2, \ldots, N-1$.
8. ***Объект А*** шифрует данные, показаны в виде последовательности чисел M_i по формуле: $C_i = M_i^{K_в} \bmod N$, и отправляет криптограмму $C_1, C_2, \ldots, C_i \ldots$ объекту В.
9. ***Объект В*** расшифровывает криптограмму $C_1, C_2, \ldots, C_i \ldots$ используя секретный ключ $к_с$ по формуле: $M_i = C_i^{K_с} \bmod N$.

Пример: шифрование сообщения

Действия объекта В:

- Берет P = 3, Q = 11.
- Берет модуль N = P × Q = 3 × 11 = 33.
- Берет значение функции Эйлера для N = 33: **φ(N) = (P-1) × (Q-1)** = 2 × 10 = 20.
- Берет в качестве открытого ключа $K_в$ произвольное число с учетом условия: $1 < K_в \leq \varphi(N)$, **т.е.** любое число от 1 до 20 при этом **НОД** $(K_в, 20) = 1$, допустим $K_в = 7$.
- Решаем значение секретного ключа $к_с$ используя алгоритм Евклида
  $(K_в * к_с) \bmod \varphi(N) = 1$, т.е
  $(к_с * 7) \bmod 20 = 1$ следовательно $(к_с * 7) = 20*n+1$, где n=0, 1, 2,…
  $к_с * 7 = 21$
  $к_с = 3$.
- Передает объекту А пару чисел (7, 33).

Действия объекта А:

- Составляет шифруемое сообщение.
- Составляет алфавит как последовательность целых чисел в диапазоне 0…32. Допустим: пробел – 0, буква А представляется как число 1, буква Б это 2 и В = 3. Припустим что сообщение ВАБ можно показать как последовательность числе 312, то есть $M_1 = 3$, $M_2 = 1$, $M_3 = 2$.
- Шифрует сообщение, M используя ключ $K_в = 7$ и N = 33 по формуле: $C_i = M_i^{K_в} \bmod N = M_i^7 \bmod 33$.
  Получает:
  - $C_i = 3^7 \bmod 33 = 2187 \bmod 33 = 9$
  - $C_i = 1^7 \bmod 33 = 1 \bmod 33 = 1$
  - $C_i = 2^7 \bmod 33 = 128 \bmod 33 = 29$
- Передает объекту В криптограмму: $C_1, C_2, C_3 = 9, 1, 29$.

Действия объекта В:

- Расшифровывает принятую криптограмму C_1, C_2, C_3 используя секретный ключ $к_с = 3$ по формуле: $\mathbf{M_i = C_i^{K_c} \bmod N} = C_i^3 \bmod 33$
  - $M_1 = 9^3 \bmod 33 = 729 \bmod 33 = 3$.
  - $M_2 = 1^3 \bmod 33 = 1 \bmod 33 = 1$.
  - $M_2 = 29^3 \bmod 33 = 24389 \bmod 33 = 2$.
- Сопоставим каждому числу M_i букву – получим ВАБ.

Объект получил исходное сообщение, которое послал объект А.

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.

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

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

Составляющие учебной работы	Сумма баллов	Учебная деятельность студента	Оценка в аттестации	Баллы
Текущая учебная работа в семестре	**80**	Посещение занятий по расписанию.	**1-2 балл** посещение 1 занятия	9 - 18
		Лабораторные работы	**2 балла** - посещение 1 практического или лабораторного занятия и выполнение работы на 51-65% **3 балла** - посещение 1 практического или лабораторного занятия и выполнение	18 - 36

			работы на 66-85% **4 балла** – посещение 1 занятия и существенный вклад на занятии в работу всей группы, самостоятельность и выполнение работы на 86-100%	
		Контрольная работа	**24 балла** (пороговое значение) **46 баллов** (максимальное значение)	24-46
Итого по текущей работе в семестре				51 - 100
Промежуточная аттестация (зачет)	**20** (100 баллов приведенной шкалы)	Теоретическая часть	**3 балла** (пороговое значение) **10 баллов** (максимальное значение)	3 - 10
		Практическая часть	**7 баллов** (пороговое значение) **10 баллов** (максимальное значение)	7 - 10
Итого по промежуточной аттестации (зачету)				(51 – 100% по приведенной шкале) 10 – 20 б.
Суммарная оценка по дисциплине/ Сумма баллов по 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

3. Мельников, В. П. Информационная безопасность и защита информации [Текст] : учебное пособие для вузов / В. П. Мельников. - 4-е издание, стереотипное. - Москва : Академия, 2009. - 336 с. - (Высшее профессиональное образование : Информатика и вычислительная техника). - Гриф УМО "Допущено". Количество: 30

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. Каратунова, Н. Г. Защита информации. Курс лекций [Электронный ресурс] : учебное пособие / Н. Г. Каратунова. – Электрон. текстов. данные. - Краснодар: КСЭИ, 2014. - 188 с. - Режим доступа: http://znanium.com/bookread2.php?book=503511

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.

Методические указания размещены по адресу: https://skado.dissw.ru/table/#faculty-ed_bachelor-20

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

Методы и средства защиты информации	303 Компьютерный класс. Учебная аудитория (мультимедийная) для проведения занятий: - семинарского (практического) типа; - групповых и индивидуальных консультаций; - текущего контроля и промежуточной аттестации. Специализированная (учебная) мебель: доска маркерно-меловая, столы компьютерные, стулья. Оборудование для презентации учебного материала: стационарное - ноутбук преподавателя, экран, проектор. Оборудование: компьютеры для обучающихся (11 шт.). Используемое программное обеспечение: MSWindows (MicrosoftImaginePremium 3 year по сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.), LibreOffice (свободно распространяемое ПО), BloodshedDevC++ 4.9.9.2 (свободно распространяемое ПО), FoxitReader (свободно распространяемое ПО), Firefox 14 (свободно распространяемое ПО), Java (бесплатная версия), MicrosoftSQLServer 2008 (MicrosoftImaginePremium 3 yearпо сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.), OpenProject (бесплатная версия), Opera 12 (свободно распространяемое ПО), Яндекс.Браузер (отечественное свободно распространяемое ПО), OracleVMVirtualBox (бесплатная версия), Scilab(свободно распространяемое ПО), SWI-Prolog(свободно распространяемое ПО), UML-диаграммы (бесплатная версия), Denwer (свободно распространяемое ПО), Eclipse(свободно распространяемое ПО), FreePascal(свободно распространяемое ПО), Geany(свободно распространяемое ПО), Kompozer(свободно распространяемое ПО), Lazarus(свободно распространяемое ПО), Pascal ABC.NET(свободно распространяемое ПО), Blender(свободно распространяемое ПО), Qucs(свободно распространяемое ПО), Gimp 2(свободно распространяемое ПО), Paint.NET(свободно распространяемое ПО), Dia(свободно распространяемое ПО), Qcad(свободно распространяемое ПО), Audacity(свободно	654027, Кемеровская область - Кузбасс, г. Новокузнецк, пр-кт Пионерский, д.13, пом. 2

	распространяемое ПО), AdobeReaderXI(свободно распространяемое ПО), WinDjView(свободно распространяемое ПО), WxMaxima(свободно распространяемое ПО), kturtle(свободно распространяемое ПО). Интернет с обеспечением доступа в ЭИОС.	

Составитель (и): Дробахина А.Н., доцент.

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