МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Горно-Алтайский государственный университет» (ФГБОУ ВО ГАГУ, ГАГУ, Горно-Алтайский государственный университет)

Информационная безопасность

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **кафедра математики, физики и информатики**

Учебный план 02.03.01_2021_621.plx
02.03.01 Математика и компьютерные науки
Математическое и программное обеспечение компьютерных сетей

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **6 ЗЕТ**

Часов по учебному плану 216
в том числе:
аудиторные занятия 36
самостоятельная работа 143,1
часов на контроль 34,75

Виды контроля в семестрах:
экзамены 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	15 3/6			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Лабораторные	18	18	18	18
Консультации (для студента)	0,9	0,9	0,9	0,9
Контроль самостоятельной работы при проведении аттестации	0,25	0,25	0,25	0,25
Консультации перед экзаменом	1	1	1	1
В том числе инт.	8	8	8	8
Итого ауд.	36	36	36	36
Контактная работа	38,15	38,15	38,15	38,15
Сам. работа	143,1	143,1	143,1	143,1
Часы на контроль	34,75	34,75	34,75	34,75
Итого	216	216	216	216

Программу составил(и):
кандидат физико-математических наук, доцент, Кайгородов Евгений Владимирович

Рабочая программа дисциплины
Информационная безопасность

разработана в соответствии с ФГОС:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 02.03.01 Математика и компьютерные науки (приказ Минобрнауки России от 23.08.2017 г. № 807)

составлена на основании учебного плана:
02.03.01 Математика и компьютерные науки
утвержденного учёным советом вуза от 10.06.2021 протокол № 7.

Рабочая программа утверждена на заседании кафедры
кафедра математики, физики и информатики

Протокол от 22.06.2021 протокол № 10

И. о. зав. кафедрой Часовских Николай Сергеевич

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры
кафедра математики, физики и информатики

Протокол от 8 июня 2023 г. № 11
И. о. зав. кафедрой: Богданова Рада Александровна

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	*Цели:* формирование у студентов системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.
1.2	*Задачи:* Задачи изучения дисциплины продиктованы требованием формирования у студентов системного подхода к решению проблем информационной безопасности: освоение основных понятий и терминологии информационной безопасности; знакомство с угрозами, которым подвергается информация, а также классификацией этих угроз и их анализом; изучение организационно-административных и технических методов и средств защиты информации; изучение криптографических методов защиты информации; изучение нормативно-законодательной базы и стандартов информационной безопасности и защиты информации; изучение моделей информационной безопасности; обеспечение безопасности автоматизированных систем; обеспечение компьютерной и сетевой безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Алгебра
2.1.2	Теория чисел
2.1.3	Правоведение
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Методика обучения информатике и ИКТ в школе

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
УК-2: Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
ИД-1.УК-2: Знает необходимые для осуществления профессиональной деятельности правовые нормы
знает проблемы и тенденции развития в области информационной безопасности, состояние законодательной базы информационной безопасности, роль и задачи информационной безопасности на предприятии, техническое и программное обеспечение для решения задач информационной безопасности
ИД-3.УК-2: Имеет практический опыт применения нормативной базы и решения задач в области избранных видов профессиональной деятельности
способен обеспечивать безопасность и целостность данных ИС и технологий, применять навыки организации защиты информации от утечки по техническим каналам на объектах информатизации, разработки политики информационной безопасности организации
ОПК-5: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности
ИД-1.ОПК-5: Знает современные информационные технологии
знает средства и методы предотвращения и обнаружения вторжений, виды угроз ИС и методы обеспечения информационной безопасности (принципы обеспечения информационной безопасности), основы методов и алгоритмов обеспечения информационной безопасности
ИД-2.ОПК-5: Умеет выбирать современные информационные технологии необходимые для решения профессиональных задач
умеет выявлять угрозы информационной безопасности, оценивать защищенность информационных ресурсов, формулировать и решать задачи проектирования защищенных профессионально-ориентированных информационных систем с использованием различных методов и решений
ИД-3.ОПК-5: Владеет навыками применения современных информационных технологий для решения профессиональных задач
владеет инструментальными средствами защиты информации, методами расчета и инструментального контроля показателей технической защиты информации, методами обеспечения информационной безопасности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)							
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**	**Инте ракт.**	**Примечание**
	Раздел 1. Методы и средства организационно-правовой защиты информации						
1.1	Введение в информационную безопасность /Лек/	6	2	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	0	
1.2	Правовое обеспечение информационной безопасности /Лек/	6	2	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	2	лекция-визуализация
1.3	Организационное обеспечение информационной безопасности /Лек/	6	2	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	0	
1.4	Информационная безопасность деятельности общества. Организационное и правовое обеспечение информационной безопасности /Лаб/	6	2	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	0	
1.5	Анализ Доктрины информационной безопасности Российской Федерации /Ср/	6	28,5	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	0	
1.6	Анализ защищенности объекта защиты информации /Ср/	6	34,2	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	0	
	Раздел 2. Методы и средства инженерно-технической защиты информации						
2.1	Технические средства и методы защиты информации /Лек/	6	2	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	0	

2.2	Программно-аппаратные средства и методы обеспечения информационной безопасности /Лек/	6	2	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	2	проблемная лекция
2.3	Криптографические методы защиты информации /Лек/	6	8	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	0	
2.4	Использование криптографических средств защиты информации /Лаб/	6	8	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	0	
2.5	Реализация работы инфраструктуры открытых ключей /Лаб/	6	2	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	0	
2.6	Средства стеганографии для защиты информации /Лаб/	6	2	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	2	кластер
2.7	Настройка безопасного сетевого соединения /Лаб/	6	2	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	0	
2.8	Антивирусные средства защиты информации /Лаб/	6	2	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	2	круглый стол
2.9	Электронные ключи, электронные замки. Средства для оценки защищенности /Ср/	6	14	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	0	
2.10	Стандарты шифрования ГОСТ 28147-89, DES, AES, RSA, PGP. Стандарты электронно-цифровой подписи ГОСТ 34.10-04, ГОСТ 34.10-2001, DSS /Ср/	6	16,8	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	0	

2.11	Электронные платежи. Электронный кошелек /Ср/	6	16,8	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	0	
2.12	Средства идентификации. Биометрическая идентификация /Ср/	6	16,6	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	0	
2.13	Удостоверяющий центр. Использование сертификатов ЭЦП для работы в сети. Использование SSL, TLS /Ср/	6	16,2	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	0	
	Раздел 3. Промежуточная аттестация (экзамен)						
3.1	Подготовка к экзамену /Экзамен/	6	34,75	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	0	
3.2	Контроль СР /КСРАтт/	6	0,25	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	0	
3.3	Контактная работа /КонсЭк/	6	1	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	0	
	Раздел 4. Консультации						
4.1	Консультация по дисциплине /Конс/	6	0,9	ИД-1.УК-2 ИД-3.УК-2 ИД-1.ОПК-5 ИД-2.ОПК-5 ИД-3.ОПК-5	Л1.1 Л1.2Л2.1	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Пояснительная записка

1. Назначение фонда оценочных средств. Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины Информационная безопасность

2. Фонд оценочных средств включает контрольные материалы для проведения текущего контроля и промежуточной аттестации в форме вопросов для входного контроля, первой и второй текущей аттестации, примерной тематики рефератов и вопросов к промежуточной аттестации

5.2. Оценочные средства для текущего контроля

Примерные вопросы для входного контроля, первой и второй промежуточной аттестации

Критерии оценки для всех аттестаций, проходящих в форме компьютерного тестирования.
менее 60% - неудовлетворительно
60%-74 %- удовлетворительно
75%-89%- хорошо
90% и более - отлично

Входной контроль
1. Кодирование – это

Выберите один ответ:
a. написание программы
b. преобразование обычного, понятного текста в код
c. преобразование

2.Что требуется для восстановления зашифрованного текста

Выберите один ответ:
a. вектор
b. ключ
c. матрица

3.Что требуется для восстановления зашифрованного текста

Выберите один ответ:
a. вектор
b. ключ
c. матрица

4.Компьютерные вирусы

Выберите один ответ:
a. являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.
b. являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.
c. вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам
d. это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров

5.Межсетевой экран (брандмауэр)

Выберите один ответ:
a. программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами
b. являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.
c. являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.
d. это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

6.Государственная тайна это

Выберите один ответ:
a. защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной, оперативно-розыскной деятельности, распространение которых может нанести ущерб государству.
b. это сведения, которые становятся известными какому-либо лицу в связи с выполнением своих профессиональных обязанностей и которые он не имеет права ни распространять, ни использовать в своих интересах
c. режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

7.Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются

Выберите один ответ:
a. коды
b. пароли
c. анкеты
d. ярлыки

8.Наиболее распространены средства воздействия на сеть офиса:

Выберите один ответ:
a. Слабый трафик, информационный обман, вирусы в интернет
b. Компьютерные сбои, изменение администрирования, топологии
c. Вирусы в сети, логические мины (закладки), информационный перехват

9.Наиболее распространены средства воздействия на сеть офиса:

Выберите один ответ:
a. Компьютерные сбои, изменение администрирования, топологии
b. Слабый трафик, информационный обман, вирусы в интернет
c. Вирусы в сети, логические мины (закладки), информационный перехват

10.Наиболее распространены угрозы информационной безопасности сети

Выберите один ответ:
a. Моральный износ сети, инсайдерство
b. Сбой (отказ) оборудования, нелегальное копирование данных
c. Распределенный доступ клиент, отказ оборудования

11.Окончательно, ответственность за защищенность данных в компьютерной сети несет:

Выберите один ответ:
a. Пользователь сети
b. Владелец сети
c. Администратор сети

12.Политика безопасности в системе (сети) – это комплекс:

Выберите один ответ:
a. Инструкций, алгоритмов поведения пользователя в сети
b. Нормы информационного права, соблюдаемые в сети
c. Руководств, требований обеспечения необходимого уровня безопасности

13.Электронно-цифровая подпись

Выберите один ответ:
a. это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки
b. программно-аппраратное устройство
c. электронный ключ

Первая промежкточная аттестация
1.Компьютерные вирусы

Выберите один ответ:
a. вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам
b. являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.
c. это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров
d. являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

2.Межсетевой экран (брандмауэр)

Выберите один ответ:
a. это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

b. программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами
c. являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.
d. являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

3.Кодирование – это

Выберите один ответ:
a. написание программы
b. преобразование обычного, понятного текста в код
c. преобразование

4.Что требуется для восстановления зашифрованного текста

Выберите один ответ:
a. вектор
b. ключ
c. матрица

5.Шифрование – это…

Выберите один ответ:
a. совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств
b. способ изменения сообщения или другого документа, обеспечивающее искажение его содержимого
c. удобная среда для вычисления конечного пользователя

6.Расшифруйте текст

отсштфрсти тцтефдкисми
N=4

7.Наиболее распространены средства воздействия на сеть офиса:

Выберите один ответ:
a. Компьютерные сбои, изменение администрирования, топологии
b. Вирусы в сети, логические мины (закладки), информационный перехват
c. Слабый трафик, информационный обман, вирусы в интернет

8.Наиболее распространены угрозы информационной безопасности сети

Выберите один ответ:
a. Моральный износ сети, инсайдерство
b. Распределенный доступ клиент, отказ оборудования
c. Сбой (отказ) оборудования, нелегальное копирование данных

9.Окончательно, ответственность за защищенность данных в компьютерной сети несет:

Выберите один ответ:
a. Администратор сети
b. Пользователь сети
c. Владелец сети

10.Подписи, созданные с использованием стандарта ГОСТ Р3410-94, являются рандомизированными, так как

Выберите один ответ:
a. для одинаковых сообщений с использованием одного и того же закрытого ключа каждый раз будут создаваться разные подписи
b. для одинаковых сообщений с использованием разных закрытых ключей каждый раз будут создаваться разные подписи
c. для разных сообщений с использованием одного и того же закрытого ключа каждый раз будут создаваться разные подписи

11.олитика безопасности в системе (сети) – это комплекс:

Выберите один ответ:
a. Руководств, требований обеспечения необходимого уровня безопасности
b. Инструкций, алгоритмов поведения пользователя в сети
c. Нормы информационного права, соблюдаемые в сети

12.Что общего имеют все методы шифрования с закрытым ключом?

Выберите один ответ:
a. в них для операций шифрования и расшифрования используется два разных ключа – открытый и закрытый
b. в них для шифрования и расшифрования информации используется один и тот же ключ
c. в них для шифрования информации используется один ключ, а для расшифрования – другой ключ

13.Электронно-цифровая подпись

Выберите один ответ:
a. это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки
b. программно-аппраратное устройство
c. электронный ключ

Вторая промежуточная аттестация

1.Поставьте в соответствие термину его описание

Блокировщики

Ответ 1
Выберите...
Ревизоры

Ответ 2
Выберите...
Полифаги

Ответ 3

2.Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ)

Выберите один ответ:
a. МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты
b. МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения
c. МЭ работают только на сетевом уровне, а СОВ – еще и на физическом

3.Политика безопасности в системе – это комплекс

Выберите один ответ:
a. Нормы информационного права, соблюдаемые в сети
b. Инструкций, алгоритмов поведения пользователя в сети
c. Руководств, требований обеспечения необходимого уровня безопасности

4.Свойство информации, наиболее актуальными при обеспечении информационной безопасности является

Выберите один ответ:
a. Доступность
b. Актуальность
c. Целостность

5.Утечкой информации в системе называется ситуация, характеризуемая

Выберите один ответ:
a. Изменением формы информации
b. Изменением содержания информации
c. Потерей данных в системе

6.ервисы безопасности

Выберите один или несколько ответов:

a. идентификация и аутентификация
b. инверсия паролей
c. обеспечение безопасного восстановления
d. кэширование записей
e. контроль целостности
f. экранирование
g. шифрование
h. регулирование конфликтов

7.К категории вирусов не относится

Выберите один ответ:
a. type_ вирусы
b. файловые вирусы
c. сетевые вирусы
d. загрузочные вирусы

8.Заражению компьютерными вирусами могут подвергнуться

Выберите один ответ:
a. звуковые файлы
b. видеофайлы
c. программы и документы
d. графические файлы

9.Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей

Выберите один ответ:
a. нигерийские письма
b. источник слухов
c. фишинг
d. черный пиар

10.Интернет черви это

Выберите один ответ:
a. Операция преобразования знаков или групп знаков одной знаковой системы или группы знаков в другой знаковой системе
b. Распространяются в компьютерной сети в воженных почтовых сообщениях
c. Приложение для операционной системы widdows

11.Расшифруйте текст Шифр Цезаря сдвиг 3

жлччзузрщлгщлв

12.Расшифруйте текст. Шифр Цезаря сдвиг 1

йнрмйлбуйгоьк

13.Расшифруйте текст . Шифр Цезаря сдвиг 2

мвскфвнкйвшкб

14.Расшифруйте текст. Шифр Виженера. Ключ бур

лвьмуспдрчьяоьву

15.Расшифруйте текст. Шифр Цезаря сдвиг 3

лржцнщлсррюм

5.3. Темы письменных работ (эссе, рефераты, курсовые работы и др.)

Темы сообщений и докладов

Критерии оценки
- оценка «отлично» выставляется студенту, если он полно раскрыл тему доклада без дополнений или если в ответе

присутствуют небольшие (не принципиальные) отклонения или наводящие (уточняющие) вопросы преподавателя;
- оценка «хорошо» выставляется студенту, если он полно раскрыл основные аспекты доклада, но упустил некоторые важные детали или если в ответе присутствуют небольшие (не принципиальные) отклонения или наводящие (уточняющие) вопросы преподавателя;
- оценка «удовлетворительно» выставляется студенту, если он не полно раскрыл тему доклада, используя лишь общие понятия или если в ответе присутствуют большие отклонения или наводящие (уточняющие) вопросы преподавателя;
- оценка «неудовлетворительно» ставится при невыполнении студентом реферата или не владении материалом в докладе.
-оценка «зачтено» - реферат выполнен и раскрывает тему, студент владеет знаниями материала.
-оценка «не зачтено» - реферат не выполнен или студент не владеет материалом, отраженным в тексте.

1. Системы идентификации по индивидуальным характеристикам человека (биометрическая идентификация: по физиологическим параметрам и характеристикам, по особенностям поведения человека).
2. Стеганография. Принципы и алгоритмы.
3. Принципы и методы защиты оптических дисков.
4. Электронные деньги.
5. Смарт-карты.
6. Протоколы SSL (Secure Socket Layer) и TLS (Transport Layer Security).
7. Шифропанки.
8. Аппаратное шифрование.
9. Криптография на эллиптических кривых.
10. Защита данных в СУБД.
11. Защита телефонных разговоров (PGPfone).
12. Устройства Touch-memory.
13. DoS-атаки.
14. Акустические каналы утечки информации (радиопередающие средства, ИК передатчики, закладки, диктофоны, проводные микрофоны, «телефонное ухо»).
15. Линейный и дифференциальный криптоанализ.
16. «Шаг младенца, шаг великана» - метод для вычисления обратной функции (методы взлома, основанные на дискретном логарифмировании).
17. Стандарты безопасности.
18. Настройка безопасности почтовых клиентов Outlook Express и MS Office Outlook.

5.4. Оценочные средства для промежуточной аттестации

Вопросы к экзамену

Критерии оценки
Для устных ответов определяются следующие критерии оценок:

Оценка «5» выставляется, если студент:
- полно раскрыл содержание материала в объеме, предусмотренном программой и учебником;
- изложил материал грамотным языком в определенной логической последовательности, точно используя математическую и специализированную терминологию и символику;
- правильно выполнил графическое изображение алгоритма и иные чертежи и графики, сопутствующие ответу;
- показал умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации при выполнении практического задания;
- продемонстрировал усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость используемых при ответе умений и навыков;
- отвечал самостоятельно без наводящих вопросов преподавателя.
Возможны одна-две неточности при освещении второстепенных вопросов или в выкладках, которые ученик легко исправил по замечанию учителя.

Оценка «4» выставляется, если:
ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков:
- в изложении допущены небольшие пробелы, не исказившие логического и информационного содержания ответа;
- допущены один-два недочета при освещении основного содержания ответа, исправленные по замечанию учителя;
- допущены ошибка или более двух недочетов при освещении второстепенных вопросов или в выкладках, легко исправленные по замечанию преподавателя.

Оценка «3» выставляется, если:
- неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения программного материала, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, чертежах, блок-схем и выкладках, исправленные после нескольких наводящих вопросов преподавателя;
- студент не справился с применением теории в новой ситуации при выполнении практического задания, но выполнил задания обязательного уровня сложности по данной теме,
- при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков.

Оценка «2» выставляется, если:
- не раскрыто основное содержание учебного материала;
- обнаружено незнание или непонимание учеником большей или наиболее важной части учебного материала,
- допущены ошибки в определении понятий, при использовании терминологии, в чертежах, блок-схем и иных выкладках, которые не исправлены после нескольких наводящих вопросов преподавателя.

Оценка зачтено выставляется если студент получил оценку удовлетворительно и выше, в противном случае- оценка незачтено

1. Цели государства в области обеспечения информационной безопасности.
2. Основные нормативные акты РФ, связанные с правовой защитой информации.
3. Виды компьютерных преступлений.
4. Способы и механизмы совершения информационных компьютерных преступлений.
5. Основные параметры и черты информационной компьютерной преступности в России.
6. Компьютерный вирус. Основные виды компьютерных вирусов.
7. Методы защиты от компьютерных вирусов.
8. Типы антивирусных программ.
9. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
10. Основные угрозы компьютерной безопасности при работе в сети Интернет.
11. Виды защищаемой информации.
12. Государственная тайна как особый вид защищаемой информации.
13. Конфиденциальная информация.
14. Система защиты государственной тайны.
15. Правовой режим защиты государственной тайны.
16. Защита интеллектуальной собственности средствами патентного и авторского права.
17. Международное законодательство в области защиты информации.
18. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
19. Симметричные шифры.
20. Асимметричные шифры.
21. Криптографические протоколы.
22. Криптографические хэш-функции.
23. Электронная цифровая подпись.
24. Организационное обеспечение информационной безопасности.
25. Служба безопасности организации.
26. Методы защиты информации от утечки в технических каналах.
27. Инженерная защита и охрана объектов.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Эл. адрес
Л1.1	Сычев Ю. Н.	Стандарты информационной безопасности. Защита и обработка конфиденциальных документов: учебное пособие	Саратов: Вузовское образование, 2018	http://www.iprbookshop.ru/72345.html
Л1.2	Филиппов Б.И., Шерстнева О.Г.	Информационная безопасность. Основы надежности средств связи: учебник	Саратов: Ай Пи Эр Медиа, 2019	http://www.iprbookshop.ru/80290.html

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Эл. адрес
Л2.1	Фомин Д. В.	Защита информации: специализированные аттестованные программные и программно-аппаратные средства: практикум	Саратов: Вузовское образование, 2021	https://www.iprbookshop.ru/110329.html

6.3.1 Перечень программного обеспечения

6.3.1.1	Moodle
6.3.1.2	Adobe Reader
6.3.1.3	MS Office

6.3.1.4	WinDjView
6.3.1.5	Яндекс.Браузер
6.3.1.6	Google Chrome
6.3.1.7	Kaspersky Endpoint Security для бизнеса СТАНДАРТНЫЙ
6.3.1.8	MS WINDOWS
6.3.1.9	NVDA
6.3.2 Перечень информационных справочных систем	
6.3.2.1	Межвузовская электронная библиотека
6.3.2.2	Электронно-библиотечная система IPRbooks
6.3.2.3	База данных «Электронная библиотека Горно-Алтайского государственного университета»

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ		
	проблемная лекция	
	лекция-визуализация	
	кластер	
	круглый стол	

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)		
Номер аудитории	**Назначение**	**Основное оснащение**
209 Б1	Компьютерный класс. Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Помещение для самостоятельной работы	Маркерная ученическая доска, экран, мультимедиапроектор, посадочные места обучающихся (по количеству обучающихся), рабочее место преподавателя, компьютеры с доступом в Интернет

102 Б2	Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Рабочее место преподавателя. Посадочные места для обучающихся (по количеству обучающихся), 2 шкафа для учебных пособий, стол под ТВ. Традиционные алтайские костюмы женские (летние, зимние), традиционные костюмы мужские (летние, зимние), традиционные алтайские шапки войлочные (летние), традиционные шапки меховые (лисьи камусы), традиционные шапки из шкуры (мерлушка), лекала: лекала шапок лекала платья лекала чегедека (традиционного платья) лекала традиционной обуви из кожи расходные материалы: лисьи камусы мелушка войлок шерсть кожа разноцветная ножи для резки кожи ножницы для резки кожи шило Шерсть для валяния – в ассортименте Пленка пупырчатая Коврик бамбуковый, ф - А3 Мыло жидкое Чаша пластмассовая, глубокая для мыльного раствора Сетка москитная Поролон листовой толстый Губка хозяйственная, автомобильная Иглы для фальцевания (грубая, средняя, тонкая) Ножницы Нитки швейные Иглы швейные с большим ушком Рамки, ф- А4 для шерстяной акварели Рамка ткацкая Бисер Бусины Ленточки Пуговицы

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по освоению дисциплин (модулей)

Лекции, с одной стороны – это одна из основных форм учебных занятий в высших учебных заведениях, представляющая собой систематическое, последовательное устное изложение преподавателем определенного раздела конкретной науки или учебной дисциплины, с другой – это особая форма самостоятельной работы с учебным материалом. Лекция не заменяет собой книгу, она только подталкивает к ней, раскрывая тему, проблему, выделяя главное, существенное, на что следует обратить внимание, указывает пути, которым нужно следовать, добиваясь глубокого понимания поставленной проблемы, а не общей картины.

Работа на лекции – это сложный процесс, который включает в себя такие элементы как слушание, осмысление и собственно конспектирование. Для того, чтобы лекция выполнила свое назначение, важно подготовиться к ней и ее записи еще до прихода преподавателя в аудиторию. Без этого дальнейшее восприятие лекции становится сложным. Лекция в университете рассчитана на подготовленную аудиторию. Преподаватель излагает любой вопрос, ориентируясь на те знания, которые должны быть у студентов, усвоивших материал всех предыдущих лекций.Важно научиться слушать преподавателя во время лекции, поддерживать непрерывное внимание к выступающему.

Однако, одного слушания недостаточно. Необходимо фиксировать, записывать тот поток информации, который сообщается во время лекции – научиться вести конспект лекции, где формулировались бы наиболее важные моменты, основные положения, излагаемые лектором. Для ведения конспекта лекции следует использовать тетрадь. Ведение конспекта на листочках не рекомендуется, поскольку они не так удобны в использовании и часто теряются. При оформлении конспекта лекции необходимо оставлять поля, где студент может записать свои собственные мысли, возникающие параллельно с мыслями, высказанными лектором, а также вопросы, которые могут возникнуть в процессе слушания, чтобы получить на них ответы при самостоятельной проработке материала лекции, при изучении рекомендованной литературы или непосредственно у преподавателя в конце лекции. Составляя конспект лекции, следует оставлять значительный интервал между строчками. Это связано с тем, что иногда возникает необходимость вписать в первоначальный текст лекции одну

или несколько строчек, имеющих принципиальное значение и почерпнутых из других источников. Расстояние между строками необходимо также для подчеркивания слов или целых групп слов (такое подчеркивание вызывается необходимостью привлечь внимание к данному месту в тексте при повторном чтении). Обычно подчеркивают определения, выводы.
Также важно полностью без всяких изменений вносить в тетрадь схемы, таблицы, чертежи и т.п., если они предполагаются в лекции. Для того, чтобы совместить механическую запись с почти дословным фиксированием наиболее важных положений, можно использовать системы условных сокращений. В первую очередь сокращаются длинные слова и те, что повторяются в речи лектора чаще всего. При этом само сокращение должно быть по возможности кратким.
Семинарские (практические) занятия Самостоятельная работа студентов по подготовке к семинарскому (практическому) занятию должна начинаться с ознакомления с планом семинарского (практического) занятия, который включает в себя вопросы, выносимые на обсуждение, рекомендации по подготовке к семинару (практическому занятию), рекомендуемую литературу к теме. Изучение материала следует начать с просмотра конспектов лекций. Восстановив в памяти материал, студент приводит в систему основные положения темы, вопросы темы, выделяя в ней главное и новое, на что обращалось внимание в лекции. Затем следует внимательно прочитать соответствующую главу учебника.
Для более углубленного изучения вопросов рекомендуется конспектирование основной и дополнительной литературы. Читая рекомендованную литературу, не стоит пассивно принимать к сведению все написанное, следует анализировать текст, думать над ним, этому способствуют записи по ходу чтения, которые превращают чтение в процесс. Записи могут вестись в различной форме: развернутых и простых планов, выписок (тезисов), аннотаций и конспектов.
Подобрав, отработав материал и усвоив его, студент должен начать непосредственную подготовку своего выступления на семинарском (практическом) занятии для чего следует продумать, как ответить на каждый вопрос темы.
По каждому вопросу плана занятий необходимо подготовиться к устному сообщению (5-10 мин.), быть готовым принять участие в обсуждении и дополнении докладов и сообщений (до 5 мин.).
Выступление на семинарском (практическом) занятии должно удовлетворять следующим требованиям: в нем излагаются теоретические подходы к рассматриваемому вопросу, дается анализ принципов, законов, понятий и категорий; теоретические положения подкрепляются фактами, примерами, выступление должно быть аргументированным.
Лабораторные работы являются основными видами учебных занятий, направленными на экспериментальное (практическое) подтверждение теоретических положений и формирование общепрофессиональных и профессиональных компетенций. Они составляют важную часть теоретической и профессиональной практической подготовки.
В процессе лабораторной работы как вида учебного занятия студенты выполняют одно или несколько заданий под руководством преподавателя в соответствии с изучаемым содержанием учебного материала.
При выполнении обучающимися лабораторных работ значимым компонентом становятся практические задания с использованием компьютерной техники, лабораторно - приборного оборудования и др. Выполнение студентами лабораторных работ проводится с целью: формирования умений, практического опыта (в соответствии с требованиями к результатам освоения дисциплины, и на основании перечня формируемых компетенций, установленными рабочей программой дисциплины), обобщения, систематизации, углубления, закрепления полученных теоретических знаний, совершенствования умений применять полученные знания на практике.
Состав заданий для лабораторной работы должен быть спланирован с расчетом, чтобы за отведенное время они могли быть выполнены качественно большинством студентов.
При планировании лабораторных работ следует учитывать, что в ходе выполнения заданий у студентов формируются умения и практический опыт работы с различными приборами, установками, лабораторным оборудованием, аппаратурой, программами и др., которые могут составлять часть профессиональной практической подготовки, а также исследовательские умения (наблюдать, сравнивать, анализировать, устанавливать зависимости, делать выводы и обобщения, самостоятельно вести исследование, оформлять результаты).
Выполнению лабораторных работ предшествует проверка знаний студентов - их теоретической готовности к выполнению задания.
Формы организации студентов при проведении лабораторных работ: фронтальная, групповая и индивидуальная. При фронтальной форме организации занятий все студенты выполняют одновременно одну и ту же работу. При групповой форме организации занятий одна и та же работа выполняется группами по 2 - 5 человек. При индивидуальной форме организации занятий каждый студент выполняет индивидуальное задание.
Текущий контроль учебных достижений по результатам выполнения лабораторных работ проводится в соответствии с системой оценивания (рейтинговой, накопительной и др.), а также формами и методами (как традиционными, так и инновационными, включая компьютерные технологии), указанными в рабочей программе дисциплины (модуля). Текущий контроль проводится в пределах учебного времени, отведенного рабочим учебным планом на освоение дисциплины, результаты заносятся в журнал учебных занятий.
Объем времени, отводимый на выполнение лабораторных работ, планируется в соответствии с учебным планом ОПОП. Перечень лабораторных работ в РПД, а также количество часов на их проведение должны обеспечивать реализацию требований к знаниям, умениям и практическому опыту студента по дисциплине (модулю) соответствующей ОПОП.
Самостоятельная работа обучающихся– это планируемая учебная, учебно-исследовательская, научно-исследовательская работа, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.
Объем самостоятельной работы определяется учебным планом основной профессиональной образовательнойпрограммы (ОПОП), рабочей программой дисциплины (модуля).
Самостоятельная работа организуется и проводится с целью формирования компетенций, понимаемых как способность применять знания, умения и личностные качества для успешной практической деятельности, в том числе:
- формирования умений по поиску и использованию нормативной, правовой, справочной и специальной литературы, а также других источников информации;
- качественного освоения и систематизации полученных теоретических знаний, их углубления и расширения по применению на уровне межпредметных связей;

- формирования умения применять полученные знания на практике (в профессиональной деятельности) и закрепления практических умений обучающихся;
- развития познавательных способностей, формирования самостоятельности мышления обучающихся;
- совершенствования речевых способностей обучающихся;
- формирования необходимого уровня мотивации обучающихся к систематической работе для получения знаний, умений и владений в период учебного семестра, активности обучающихся, творческой инициативы, самостоятельности, ответственности и организованности;
- формирования способностей к саморазвитию (самопознанию, самоопределению, самообразованию, самосовершенствованию, самореализации и саморегуляции);
- развития научно-исследовательских навыков;
- развития навыков межличностных отношений.

К самостоятельной работе по дисциплине (модулю) относятся: проработка теоретического материала дисциплины (модуля);подготовка к семинарским и практическим занятиям, в т.ч. подготовка к текущему контролю успеваемости обучающихся(текущая аттестация); подготовка к лабораторным работам; подготовка к промежуточной аттестации (зачётам, экзаменам).

Виды, формы и объемы самостоятельной работы обучающихсяпри изучении дисциплины (модуля) определяются:
- содержанием компетенций, формируемых дисциплиной (модулем);
- спецификой дисциплины (модуля), применяемыми образовательными технологиями;
- трудоемкостью СР, предусмотренной учебным планом;
- уровнем высшего образования (бакалавриат, специалитет, магистратура, аспирантура), на котором реализуется ОПОП;
- степенью подготовленности обучающихся.

Курсовая работа является самостоятельным творческим письменным научным видом деятельности студента по разработке конкретной темы. Она отражает приобретенные студентом теоретические знания и практические навыки. Курсовая работа выполняется студентом самостоятельно под руководством преподавателя.

Курсовая работа, наряду с экзаменами и зачетами, является одной из форм контроля (аттестации), позволяющей определить степень подготовленности будущего специалиста. Курсовые работы защищаются студентами по окончании изучения указанных дисциплин, определенных учебным планом.

Оформление работы должно соответствовать требованиям. Объем курсовой работы: 25–30 страниц. Список литературы и Приложения в объем работы не входят. Курсовая работа должна содержать: титульный лист, содержание, введение, основную часть, заключение, список литературы, приложение (при необходимости). Курсовая работа подлежит рецензированию руководителем курсовой работы. Рецензия является официальным документом и прикладывается к курсовой работе.

Тематика курсовых работ разрабатывается в соответствии с учебным планом. Руководитель курсовой работы лишь помогает студенту определить основные направления работы, очертить её контуры, указывает те источники, на которые следует обратить главное внимание, разъясняет, где отыскать необходимые книги.

Составленный список источников научной информации, подлежащий изучению, следует показать руководителю курсовой работы.

Курсовая работа состоит из глав и параграфов. Вне зависимости от решаемых задач и выбранных подходов структура работы должна содержать: титульный лист, содержание, введение, основную часть; заключение; список литературы; приложение(я).

Во введении необходимо отразить: актуальность; объект; предмет; цель; задачи; методы исследования; структура работы.

Основную часть работы рекомендуется разделить на 2 главы, каждая из которых должна включать от двух до четырех параграфов.

Содержание глав и их структура зависит от темы и анализируемого материала.

Первая глава должна иметь обзорно–аналитический характер и, как правило, является теоретической.

Вторая глава по большей части раскрывает насколько это возможно предмет исследования. В ней приводятся практические данные по проблематике темы исследования.

Выводы оформляются в виде некоторого количества пронумерованных абзацев, что придает необходимую стройность изложению изученного материала. В них подводится итог проведённой работы, непосредственно выводы, вытекающие из всей работы и соответствующие выявленным проблемам, поставленным во введении задачам работы; указывается, с какими трудностями пришлось столкнуться в ходе исследования.

Правила написания и оформления курсовой работы регламентируются Положением о курсовой работе (проекте), утвержденным решением Ученого совета ФГБОУ ВО ГАГУ от 27 апреля 2017 г.