МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
КРАСНОЯРСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ
им. В.П. Астафьева
(КГПУ им. В.П. Астафьева)

Институт математики, физики и информатики
Базовая кафедра информатики и информационных технологий в образовании

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ / ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление: 44.03.05 Педагогическое образование

Профиль «Математика и информатика»

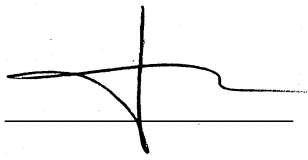
Квалификация (степень): бакалавр

Очная форма обучения

Красноярск 2016

Рабочая программа дисциплины «Защита информации / Информационная безопасность» составлена *доктором физико-математических наук, профессором кафедры ИИТвО Романовым В.А.*

Рабочая программа дисциплины обсуждена на заседании кафедры *ИИТвО протокол № 3 от 05.10.2016 г.*

Заведующий кафедрой  Пак Н.И.
(ф.и.о., подпись)

Одобрено научно-методическим советом ИМФИ
26.10.2016

Председатель  Бортновский С.В.
(ф.и.о., подпись)

Содержание

Пояснительная записка

Рабочая программа дисциплины «Защита информации / информационная безопасность» (дальше «Защита информации») для подготовки обучаемых по направлению 43.03.05 «Педагогическое образование» (уровень бакалавр) в рамках основной образовательной программы для профиля «Математика и информатика» разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования 44.03.05 «Педагогическое образование» (с двумя профилями подготовки), утвержденного 09 февраля 2016 г. № 91; и рабочим учебным планом подготовки студентов КГПУ им. В.П. Астафьева по соответствующему направлению.

Рабочая модульная программа предназначена для преподавателей и студентов, являющихся субъектами образовательного процесса в рамках данной дисциплины.

Место дисциплины в структуре образовательной программы.

Дисциплина «Защита информации» относится к вариативной части учебного плана подготовки бакалавров по программе «Педагогическое образование», профиль «Математика и информатика» и изучается на четвёртом курсе в 7 семестре. Код дисциплины в учебном плане – Б1.В.ДВ13.

Дисциплина «Защита информации» опирается на знания и способы деятельности, сформированные в предшествующих дисциплинах: «Информационные технологии в образовании», «Языки и методы программирования», «Информационная культура», «Профильное исследование в области информатики», а также естественно сочетается с материалом, излагаемым в дисциплинах «Архитектура профессионального компьютера и операционных систем», «Информационные системы и сети», читаемых в одном семестре с этой дисциплиной.

Трудоемкость дисциплины (общий объём времени, отведённого на изучение дисциплины)

По очной форме обучения общий объём часов – **72** (**2 ЗЕТ**), из них:

Аудиторных часов **44**:

Лекций – **22**

Практических работ – **22**

Часов самостоятельной работы – **28**

Контроль (экзамен) - **0**

***Цели освоения дисциплины*:**

Курс «Защита информации» направлен на введение студентов в основные проблемы, методы и технологии секьюритологии в области информационного поведения.

Основная цель курса - сформировать представление об основных аспектах информационной безопасности современного общества, о технологиях и средствах защиты информации, а также о влиянии вопросов защиты информации на процесс развития информационного общества и государства.

Курс «Защита информации» способствует углублению знаний по предметным областям:

- *Математика* (алгебра, мат. логика, и другие) – теоретическая часть курса содержит материалы, изучение которых способствует развитию математического мышления и предполагает получение некоторых дополнительных сведений по данной предметной области.
- *Обществоведение и право* – изучение законов, связанных со сферой информационной деятельности. Кроме того, систематизация знаний по общим тенденциям развития общества, в активный лексикон студентов вводятся такие понятия, как «информационное, или постиндустриальное общество», «цивилизация», «глобализация общества» и прочие.
- *История* – изучение раздела «История криптологии» подразумевает рассмотрение не только эволюции алгоритмов шифрования, но общих социальных и исторических условий, при которых происходило их создание и внедрение. Основные причины создания новых шифров и принципиально новых подходов, — это и общественно-значимые события (войны, противостояния) и события, связанные с научно-технической революцией и общим прогрессом техники и способов передачи информации (таких как изобретение письменности, книгопечатания, электричества, ЭВМ и т.д.).
- *Экономика* – рассматривается влияние защищенности информации на экономические процессы (в макро- и микроэкономике), а также коммерческое использование программной продукции, обеспечивающей информационную безопасность (мировые тенденции).
- *Английский язык* – используются аутентичные понятия и терминология (с приведением перевода), а также в некоторых заданиях примеры приведены на английском языке.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Задачи освоения дисциплины	**Планируемые результаты обучения по дисциплине** *(дескрипторы)*	**Код результата обучения** *(компетенция)*
Формирование представлений о правовых аспектах информационной безопасности, основных типах преступлений в данной сфере; формирование четкого понимания наличия ответственности при осуществлении любой информационной деятельности; создание благоприятных условий для формирования информационной культуры личности.	Понимать инструментарий и область применимости инструментов законодательного регулирования вопросов ИБ. Знать виды угроз ИБ, классификацию мер обеспечения состояния ИБ (законодательного, административного, процедурного, программно-технического уровней), основные виды преступлений в сфере информационной деятельности. Знать правовые статьи законодательства российской федерации, предусматривающие административную или уголовную ответственность за деяния, совершенные в сфере информационной деятельности. Знать методы защиты интеллектуальной собственности (законодательные, административные, программные, технические). Иметь представление о сложностях процесса законодательного регулирования ИБ, вызванных стремительным развитием современных технологий.	**ОК-6**: способность к самоорганизации и самообразованию. **ОПК-1**: готовность сознавать социальную значимость своей будущей профессии, обладать мотивацией к осуществлению профессиональной деятельности. **ОПК-2**: способностью осуществлять обучение, воспитание и развитие с учетом социальных, возрастных, психофизических и индивидуальных особенностей, в том числе особых образовательных потребностей обучающихся.
Изучение общих принципов защиты информации с помощью программных средств, теоретических обоснований алгоритмов шифрования, истории криптологии как науки; знакомство с основами симметричной и несимметричной криптографии;	Знание истории развития средств криптографии как результата борьбы в информационном пространстве. Иметь представление о ключевых элементах криптографической системы, используемом математическом аппарате, уязвимости протоколов обмена. Знать общие принципы защиты информации в компьютерных системах и телекоммуникационных сетях, теоретические обоснования основных методов защиты информации. Иметь представление о криптографических методах защиты и основных принципах функционирования симметричных и асимметричных криптосистем, о методах ограничения доступа к информации на различных уровнях.	**ОК-3**: способность использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве. **ОК-4**: способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия. **ПК-11**: готовность использовать систематизированные теоретические и практические знания для постановки и решения исследовательских задач в области образования.
Углубление знаний в областях, смежных с информатикой и информационной безопасностью, в области объектно-ориентированного программирования;	Получить опыт написания уязвимого ПО и техники эксплуатации уязвимостей. Уметь оценивать степень риска и возможный ущерб при нарушении ИБ на персональном уровне, обнаруживать вредоносное программное обеспечение и сетевые атаки, устранять последствия воздействия вредоносного программного обеспечения и сетевых атак,	**ОПК-1**: готовность сознавать социальную значимость своей будущей профессии, обладать мотивацией к осуществлению профессиональной деятельности.

иметь представление о природе уязвимостей программного обеспечения и техники их эксплуатации.	выделять конкретную проблему из ситуации, связанной с информационной безопасностью.	
Формирование общих понятий о роли информации и способах манипуляции в информационном противостоянии государств и обеспечении безопасности страны.	Иметь представление о роли ИБ с точки зрения государства. На примере конкретных кейсов изучить приёмы информационной борьбы, их значимости для государства и гражданина.	**ОПК-5**: владение основами профессиональной этики и речевой культуры.
Формирование культуры соблюдения информационной безопасности при работе на персональном рабочем месте.	Быть готовым учитывать вопросы ИБ при реализации новых образовательных программ. Использовать полученные знания и умения для анализа и проектирования безопасной информационной деятельности на законодательном и административном уровнях. Владеть специальным программным обеспечением (антивирусы, средства сетевого экранирования, средства ограничения файлового доступа и шифрования, средства для восстановления информации) для обеспечения личной информационной безопасности.	**ПК-1**: готовность реализовывать образовательные программы по предметам в соответствии с требованиями образовательных стандартов.

Особенности технологий обучения:

В курсе применяются следующие интерактивные методы и формы проведения учебных занятий: мозговой штурм; сетевая дискуссия, круглый стол в сетевом режиме; совместная экспертиза продуктов деятельности, творческие задания, эвристическая беседа.

Виды учебных действий и формы учебной деятельности в курсе проектируются релевантно образовательным результатам согласно когнитивной таксономии:


Самостоятельность, самоконтроль
Уровень
Действия
Оценка
Критическая оценка, выбор варианта, принятие решения, формулировка результатов и выводов
Синтез
Проектирование решения, конструирование, комбинирование, интегрирование, разработка
Анализ
Декомпозиция задачи, нахождение связей, обобщение, классификация, сравнение, группировка, систематизация
Применение
Применение, использование образца, экспериментирование, прогнозирование
Понимание
Объяснение, описание «своими словами», обоснование
Знание
Перечисление, определение, демонстрация, обозначение, называние (терминов, способов)
Работа вне аудитории в составе малой группы, дистанционные консультации с преподавателем
Работа в аудитории в составе малой группы, обсуждение с преподавателем

Лист согласования учебной программы с другими дисциплинами направления и ООП

на 2016/2017 учебный год

Наименование дисциплин, изучение которых опирается на данную дисциплину	Кафедра	Предложения об изменениях в дидактических единицах, временной последовательности изучения и т.д.	Принятое решение (протокол №, дата) кафедрой, разработавшей программу
Информационные системы и сети	ИИТвО		
Информационные и коммуникационные технологии в образовании	ИИТвО		

Заведующий кафедрой ИИТвО _____ Пак Н.И.

Председатель НМС ИМФИ _____ Бортновский С.В.
(ф.и.о., подпись)

05.10.2016

ТЕХНОЛОГИЧЕСКАЯ КАРТА ОБУЧЕНИЯ ДИСЦИПЛИНЕ

ЗАЩИТА ИНФОРМАЦИИ / ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление 44.03.05 «Педагогическое образование»

Профиль: «Математика и информатика»

Квалификация: бакалавр

Очная форма обучения

(общая трудоемкость 2,0 з.е.)

Наименование разделов и тем	Всего часов	Аудиторных часов				Внеаудиторных часов	Формы и метод ы контроля
		всего	лекций	семинаров	лабор-х. работ		
ВХОДНОЙ модуль							
Информатика, информация. Подходы к измерению информации, ценность информации. Дискретная математика и компьютерная алгебра. Кольца, поля, хеш-функции. Перестановки, комбинаторика. Информационные системы и компьютерные сети. Алгоритмизация и программирование. Операционные системы и классификация ПО.	4	2		2		2	Опрос.
МОДУЛЬ 1: Проблемы информационной безопасности в современном обществе.							
1. Общие вопросы информационной безопасности. Информационная модель постиндустриального общества. Ключевые документы в области информационной безопасности РФ. Уровни информационной безопасности.	6	4	2	2		2	Опрос Практическая работа 1. Доклад 1.
2. Ценность информации и инфраструктуры обеспечения информационной безопасности. Риски и ущерб. Административные, государственные и правовые аспекты информационной безопасности.	6	4	2	2		2	Опрос Практическая работа 2.

3. Юридические определения объектов защиты информации и поддерживающей инфраструктуры. Обзор мировой законодательной практики. Судебные прецеденты и ответственность за нарушение законов	6	4	2	2		2	Опрос Практическая работа 3.
ВСЕГО	18 (0.5 з.е.)	12	6	6		6	
МОДУЛЬ 2: Криптология и защита информации							
1. Принципы стеганографии. Основные понятия криптографии и криптоанализа. Симметричные и асимметричные криптосистемы. Классификации шифров и стандарты. Развитие теорий защиты информации.	6	4	2	2		2	Опрос Практическая работа 4. Доклад 2.
2. Проблемы защиты информации: с древних времен до современности. История криптологии (криптографии, стеганографии, криптоанализа).	8	6	4	2		2	Опрос Практическая работа 5.
3. Теоретические модели защиты информации. Ручные и механические докомпьютерные средства защиты информации.	6	4	2	2		2	Опрос Практическая работа 6. УНИП.
ВСЕГО	20 (0,55 з.е.)	14	8	6		6	
МОДУЛЬ 3: Безопасность компьютерных систем и сетевых технологий							
1. Программные и аппаратные угрозы информационной безопасности. Вредоносное программное обеспечение: классификации, методы профилактики и защиты.	7	4	2	2		3	Опрос Практическая работа 7.
2. Программные средства защиты информации (ограничения доступа и шифрования).	7	4	2	2		3	Опрос
3. Безопасность современных платформ (Windows, Linux, Mac). Технические аспекты информационной безопасности.	8	4	2	2		4	Опрос

4. Информационная безопасность в сетевых технологиях: протоколы, криптография, специальные программные и аппаратные средства.	8	4	2	2		4	Опрос Исследовательский реферат.
ВСЕГО	30 (0,83 з.е.)	16	8	8		14	
ИТОГОВЫЙ МОДУЛЬ							
Зачет							Оценка результатов устного зачета
Защита исследовательского реферата							Оценка результатов НИР в процессе публичной защиты.
ИТОГО:	**72 (2 з.е.)**	**44**	**22**	**22**		**28**	

СОДЕРЖАНИЕ ОСНОВНЫХ РАЗДЕЛОВ И ТЕМ ДИСЦИПЛИНЫ

ВХОДНОЙ модуль: Входной опрос и актуализация остаточных знаний по опорным дисциплинам.

Теория	Практика
Информатика, информация. Подходы к измерению информации, ценность информации. Дискретная математика и компьютерная алгебра. Кольца, поля, хеш-функции. Перестановки, комбинаторика. Информационные системы и компьютерные сети. Алгоритмизация и программирование. Операционные системы и классификация ПО.	Методы измерения количества информации. Структурное, визуальное, функциональное и объектно-ориентированное программирование.

МОДУЛЬ 1: Проблемы информационной безопасности в современном обществе.

Теория	Практика
Общие вопросы информационной безопасности. Информационная модель постиндустриального общества. Ключевые документы в области информационной безопасности РФ. Уровни информационной безопасности.	Научный анализ ведущих идей, лежащих в основе инновационных преобразований современного общества. Анализ нормативной документации в сфере ИБ.
Ценность информации и инфраструктуры обеспечения информационной безопасности. Риски и ущерб. Административные, государственные и правовые аспекты информационной безопасности.	Определение количества информации и ее ценности на основе известных методов. Анализ рисков и уязвимостей. Оценка неприемлемого ущерба.
Юридические определения объектов защиты информации и поддерживающей инфраструктуры. Обзор мировой законодательной практики. Судебные прецеденты и ответственность за нарушение законов	Анализ свода законов в области информационного права.

МОДУЛЬ 2: Криптология и защита информации.

Теория	Практика
Принципы стеганографии. Основные понятия криптографии и криптоанализа. Симметричные и асимметричные криптосистемы. Классификации шифров и стандарты. Развитие теорий защиты информации.	Моделирование криптосистем: симметричные, поточные. Моделирование криптосистем: симметричные, блочные.
Проблемы защиты информации: с древних времен до современности. История криптологии (криптографии, стеганографии, криптоанализа).	Программирование древних шифров.
Теоретические модели защиты информации. Ручные и механические докомпьютерные средства защиты информации.	Моделирование докомпьютерных средств защиты информации.

МОДУЛЬ 3: Безопасность компьютерных систем и сетевых технологий.

Теория	Практика
Программные и аппаратные угрозы информационной безопасности. Вредоносное программное обеспечение: классификации, методы профилактики и защиты.	Анализ компьютерной системы. Антивирусная защита.
Программные средства защиты информации (ограничения доступа и шифрования).	Шифрование, ЭЦП. Программные и аппаратные средства обеспечения целостности, доступности и конфиденциальности информации.
Безопасность современных платформ (Windows, Linux, Mac). Технические аспекты информационной безопасности.	Сравнительный анализ операционных систем.
Информационная безопасность в сетевых технологиях: протоколы, криптография, специальные программные и аппаратные средства.	Методы обеспечения информационной безопасности в компьютерной сети.

ИТОГОВЫЙ модуль: Защита исследовательского реферата, ЗАЧЕТ

ТЕХНОЛОГИЧЕСКАЯ КАРТА РЕЙТИНГА ДИСЦИПЛИНЫ

Наименование дисциплины	**Направление подготовки и уровень образования (бакалавриат, магистратура, аспирантура) Наименование программы/ профиля**	**Количеств з.е.**
Защита информации / Информационная безопасность	НАПРАВЛЕНИЕ: 44.03.05 «Педагогическое образование» Профиль: «Математика и информатика» Квалификация (степень): бакалавр по **очной** форме обучения	**2**
Смежные дисциплины по учебному плану		
Предшествующие:		
«Информационные технологии в образовании», «Языки и методы программирования», «Информационная культура», «Профильное исследование в области информатики»		
Последующие:		
-		

ВХОДНОЙ МОДУЛЬ			
	Форма работы	Количество баллов 10 %	
		min	max
Промежуточный рейтинг-контроль	Опрос	3	10
Итого		**3**	**10**

БАЗОВЫЙ МОДУЛЬ № 1			
	Форма работы	Количество баллов 20 %	
		min	max
Текущая работа	Лекция 1-3	3	6
	ПР 1-3	3	6
Промежуточный рейтинг-контроль	Доклад 1	3	8
Итого		**9**	**20**

БАЗОВЫЙ МОДУЛЬ № 2			
	Форма работы	Количество баллов 30 %	
		min	max
Текущая работа	Лекция 4-6	3	6

	ПР 4-6	5	8
Промежуточный рейтинг-контроль	Доклад 2	3	5
Промежуточный рейтинг-контроль	УНИП	8	10
Итого		**19**	**29**

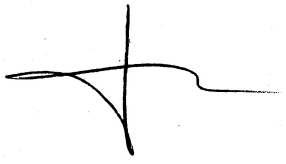
БАЗОВЫЙ МОДУЛЬ № 3			
	Форма работы	Количество баллов 40 %	
		min	max
Текущая работа	Лекция 7-10	4	8
	ПР 7	8	12
Промежуточный рейтинг-контроль	Реферат	17	21
Итого		**29**	**41**

ИТОГОВЫЙ МОДУЛЬ		
Форма работы	Количество баллов	
	min	max
Защита исследовательского реферата	0	15
Зачет	0	10
Общее количество баллов по дисциплине (по итогам изучения всех разделов, без учета дополнительного)	**60**	**100**

Соответствие рейтинговых баллов и академической оценки

Общее количество набранных баллов	*Академическая оценка*
меньше **60** или незакрытый модуль	**не зачтено**
	зачтено

ФИО преподавателя: *Романов Валерий Александрович*
Утверждено на заседании кафедры «05» октября 2016 г. Протокол № 3



Зав. кафедрой Н.И. Пак

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«Красноярский государственный педагогический университет им. В.П. Астафьева»

Институт математики, физики и информатики
(наименование института/факультета)

Кафедра-разработчик Информатики и информационных технологий в образовании
(наименование кафедры)

УТВЕРЖДЕНО
на заседании кафедры
Протокол № 3
от «05» октября 2016 г.

ОДОБРЕНО
на заседании научно-методического совета направления подготовки
Протокол № 2
от «26» октября 2016 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля и промежуточной аттестации обучающихся

«Защита информации»
(наименование дисциплины/модуля/вида практики)

44.03.05 «Педагогическое образование»
(код и наименование направления подготовки)
Профиль «Математика и информатика»
(наименование профиля подготовки/наименование магистерской программы)
бакалавр
(квалификация (степень) выпускника)

Составитель: Романов В.А., профессор кафедры ИИТО

1. **Назначение фонда оценочных средств**

1.1. **Целью** создания ФОС дисциплины «Защита информации / информационная безопасность» является установление соответствия учебных достижений запланированным результатам обучения и требованиям основной профессиональной образовательной программы, рабочей программы дисциплины.

1.2. ФОС по дисциплине решает **задачи**:

1. Управление процессом приобретения обучающимися необходимых знаний, умений, навыков и формирования компетенций, определенных в образовательных стандартах по соответствующему направлению подготовки.

2. Оценка достижений обучающихся в процессе изучения дисциплины с определением положительных/отрицательных результатов и планирование предупреждающих/корректирующих мероприятий.

3. Обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс.

4. Совершенствование процессов самоподготовки и самоконтроля обучающихся.

1.3. ФОС разработан на основании нормативных **документов**:

- Федерального государственного образовательного стандарта высшего образования по направлению подготовки 44.03.05 «Педагогическое образование» Квалификация (степень) «Бакалавр».

- Положения о формировании фонда оценочных средств для текущего контроля успеваемости, промежуточной и итоговой аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры, программам подготовки научно-педагогических кадров в аспирантуре в федеральном государственном бюджетном образовательном учреждении высшего образования «Красноярский государственный педагогический университет им. В.П. Астафьева» и его филиалах.

2. Перечень компетенций с указанием этапов их формирования в процессе изучения дисциплины/модуля/прохождения практики

2.1. **Перечень компетенций,** формируемых в процессе изучения дисциплины:

а) общекультурные:

ОК-3 - способность использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве

ОК-4 - способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия.

ОК-6 - способность к самоорганизации и самообразованию

б) общепрофессиональные:

ОПК-1 - готовность сознавать социальную значимость своей будущей профессии, обладать мотивацией к осуществлению профессиональной деятельности.

ОПК-2 - способность осуществлять обучение, воспитание и развитие с учетом социальных, возрастных, психофизических и индивидуальных особенностей, в том числе особых образовательных потребностей обучающихся

ОПК-5 - владение основами профессиональной этики и речевой культуры

в) профессиональные:

ПК-1 - готовность реализовывать образовательные программы по предметам в соответствии с требованиями образовательных стандартов.

ПК-11 - готовность использовать систематизированные теоретические и практические знания для постановки и решения исследовательских задач в области образования

2.2. **Этапы формирования и оценивания компетенций**

Компетенции формируются на раннем этапе с помощью учебного научно-исследовательского проекта (УНИП), темы которого даны в соответствующем разделе, оттачиваются при выполнении соответствующей практической работы, применяются и тестируются при написании реферата и сдаче зачёта. Ниже приведены компетенции и соответствующие темы практических работ.

Компетенция	Этап формирования компетенции	Дисциплины, практики, участвующие в формировании компетенции	Тип контроля	Оценочное средство / КИМы	
				Номер	Форма

ОК-3 - способность использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве **ПК-11** - готовность использовать систематизированные теоретические и практические знания для постановки и решения исследовательских задач в области образования	ориентировочный	Защита информации	текущий контроль	1	УНИП
	когнитивный		текущий контроль	2	практическая работа №1
	праксиологический		Промежуточная аттестация	3	реферат
	рефлексивно-оценочный		Зачёт		зачёт
ОК-4 - способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия **ОПК-5** - владение основами профессиональной этики и речевой культуры	ориентировочный	Защита информации	текущий контроль	1	УНИП
	когнитивный	Защита информации	текущий контроль	2	практическая работа №1, 2
	праксиологический	Защита информации	Промежуточная аттестация		реферат
	рефлексивно-оценочный	Защита информации	Промежуточная аттестация		зачёт

ОК-6 - способность к самоорганизации и самообразованию **ПК-1** - готовность реализовывать образовательные программы по предметам в соответствии с требованиями образовательных стандартов	ориентировочный	Защита информации	текущий контроль	1	УНИП
	когнитивный	Защита информации	текущий контроль	2	практическая работа №3, 4
	праксиологический	Защита информации	Промежуточная аттестация	3	реферат
	рефлексивно-оценочный	Защита информации	Итоговая аттестация		зачёт
ОПК-1 - готовность сознавать социальную значимость своей будущей профессии, обладать мотивацией к осуществлению профессиональной деятельности	ориентировочный	Защита информации	текущий контроль	1	УНИП
	когнитивный	Защита информации	текущий контроль	2	практическая работа №5
	праксиологический	Защита информации	Промежуточная аттестация	3	реферат
	рефлексивно-оценочный	Защита информации	Итоговая аттестация	4	зачёт
ОПК-2 - способность осуществлять обучение, воспитание и развитие с учетом социальных, возрастных, психофизических и индивидуальных особенностей, в том числе особых образовательных потребностей обучающихся	ориентировочный	Защита информации	текущий контроль	1	УНИП
	когнитивный	Защита информации	текущий контроль	2	практическая работа №6, 7
	праксиологический	Защита информации	Промежуточная аттестация	3	реферат
	рефлексивно-оценочный	Защита информации	Итоговая аттестация	4	зачёт

3. Фонд оценочных средств для промежуточной аттестации

3.1. Фонды оценочных средств включают: перечень вопросов к зачёту.

3.2. Оценочные средства

3.2.1. Оценочное средство 1 «Вопросы к зачёту»

Критерии оценивания по оценочному средству «Вопросы к зачёту»

Формируемые компетенции	Высокий уровень сформированности компетенций	Продвинутый уровень сформированности компетенций	Базовый уровень сформированности компетенций
	(20 - 23 балла) отлично	(16 - 19 баллов) хорошо	(13 - 15 баллов)* Удовлетворительно
ОК-3 - способность использовать естественнонаучные и математические знания для ориентирования в современном информационном пространстве	Обучающийся свободно использует естественнонаучные и математические знания для ориентирования в современном информационном пространстве	Обучающийся фрагментарно использует естественнонаучные и математические знания для ориентирования в современном информационном пространстве	Обучающийся использует конкретно указанные естественнонаучные и математические знания для ориентирования в современном информационном пространстве
ОК-4 - способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия	Обучающийся демонстрирует высокий уровень владения, способен вести дискуссию, изолировать и анализировать противоречия в споре, формулировать ключевые вопросы для разрешения противоречий, видеть весь текст в полном объёме со всеми перекрёстными понятийными и логическими связями.	Обучающийся демонстрирует хороший уровень владения, способен вести дискуссию, формулировать свою точку зрения в доступной и ясной форме, формировать контекст обсуждения перед началом обсуждения и/или постановки вопроса в письменной форме.	Обучающийся демонстрирует способности к письменной речевой культуре, способен ясно понимать профессиональную речь и изъясняться с использованием соответствующего понятийного и речевого аппарата с соблюдением принятых культурных и профессиональных норм.
ОК-6 - способность к самоорганизации и самообразованию	Обучающийся грамотно планирует бюджет времени и других ресурсов, свободно использует инструменты и методики самоорганизации (GTD, Pomodoro, SWAT анализ). Обучающийся способен выделять собственные дефициты, искать качественные источники знаний, обучаться самостоятельно.	Обучающийся способен оценивать бюджет времени и ресурсов, имеет понятие о инструментах и методиках самоорганизации. Обучающийся способен выделять и формулировать собственные дефициты, искать источники знаний для их заполнения.	Обучающийся имеет понятие о методиках самоорганизации и управления временем, способен выделять и конструктивно формулировать собственные дефициты. Имеет представление о методике самообучения.
ПК-1 - готовность реализовывать образовательные программы по предметам в соответствии с требованиями образовательных стандартов	Обучающийся знаком с нормативной базой и стандартами, имеет опыт работы с ними и опыт построения и/или анализа готовых программ с точки зрения соответствия стандартам. Способен самостоятельно проектировать программы в соответствие со стандартами.	Обучающийся знаком с нормативной базой и стандартами, имеет опыт работы с ними и опыт построения и/или анализа готовых программ с точки зрения соответствия стандартам.	Обучающийся знаком с нормативной базой и стандартами, имеет опыт работы с ними, опыт самостоятельного построения образовательной программы.
ПК-11 - готовность использовать	Обучающийся обоснованно и	Обучающийся использует теоретические	Обучающийся по конкретному указанию или

систематизированные теоретические и практические знания для постановки и решения исследовательских задач в области образования	целесообразно использует систематизированные теоретические и практические знания для постановки и решения исследовательских задач в области информационной безопасности	и практические знания для постановки и решения исследовательских задач в области информационной безопасности	примеру использует теоретические и практические знания для постановки и решения исследовательских задач в области информационной безопасности
ОПК-1 - готовность сознавать социальную значимость своей будущей профессии, обладать мотивацией к осуществлению профессиональной деятельности	Обучающийся демонстрирует высокий уровень знания дисциплины, её места в экономике, системе образования, общественной жизни. Владеет практическим аппаратом дисциплины, мотивирован обучать других и делиться знаниями.	Обучающийся демонстрирует высокий уровень знания дисциплины, её места в экономике, системе образования, общественной жизни. Владеет практическим аппаратом дисциплины. Способен делиться знаниями.	Обучающийся демонстрирует знание дисциплины, её места в экономике, системе образования, общественной жизни, способен продемонстрировать и объяснить практическую значимость дисциплины.
ОПК-2 - способность осуществлять обучение, воспитание и развитие с учетом социальных, возрастных, психофизических и индивидуальных особенностей, в том числе особых образовательных потребностей обучающихся	Обучающийся демонстрирует высокий уровень способности осуществлять обучение информационной безопасности, воспитание и развитие с учетом социальных, возрастных, психофизических и индивидуальных особенностей, в том числе особых образовательных потребностей обучающихся	Обучающийся демонстрирует хороший уровень способности осуществлять обучение информационной безопасности, воспитание и развитие с учетом социальных, возрастных, психофизических и индивидуальных особенностей, в том числе особых образовательных потребностей обучающихся	Обучающийся демонстрирует достаточный уровень способности осуществлять обучение информационной безопасности, воспитание и развитие с учетом социальных, возрастных, психофизических и индивидуальных особенностей, в том числе особых образовательных потребностей обучающихся
ОПК-5 - владение основами профессиональной этики и речевой культуры	Обучающийся демонстрирует высокий уровень владения, способен вести дискуссию, изолировать и анализировать противоречия в споре, формулировать ключевые вопросы для разрешения противоречий.	Обучающийся демонстрирует хороший уровень владения, способен вести дискуссию, формулировать свою точку зрения в доступной и ясной форме.	Обучающийся демонстрирует способности к речевой культуре, способен ясно понимать профессиональную речь и изъясняться с использованием соответствующего понятийного и речевого аппарата с соблюдением принятых культурных и профессиональных норм.

*Менее 13 баллов – компетенция не сформирована

4. Фонд оценочных средств для текущего контроля успеваемости

Фонды оценочных средств включает:

1) темы учебных научно-исследовательских проектов
2) семь практических работ
3) итоговую контрольную работу

4.1.1 Критерии оценивания по оценочному средству №1: выполнение учебного научно-исследовательского проекта

Критерии оценивания	Количество баллов

	(вклад в рейтинг)
Работа не выполнена или процент плагиата выше 50%.	0
Работа выполнена на уровне копирования информации из общедоступных источников со сведением.	1
Сформулирована и развита самостоятельная мысль или высказывание.	3
Основной тезис развёрнут с квалифицированным обзором литературы.	4
Присутствуют творческие решения или самостоятельность в анализе.	5
Максимальный балл	5

4.1.2 Критерии оценивания по оценочному средству №2: практические работы

Критерии оценивания	Количество баллов (вклад в рейтинг)
Работа не выполнена.	0
Не использована соответствующая специальная и/или нормативная литература, низкая верифицируемость источников.	1
Использованы ГОСТ/международные спецификации, нормативная литература.	2
Присутствует понимание предметной области, самостоятельность мышления и анализа, опора на нормативные документы.	4
Максимальный балл	4

4.1.3 Критерии оценивания по оценочному средству №3: контрольная работа: доля успешно отвеченных вопросов.

Максимальное количество баллов рейтинга: 10.

5. Учебно-методическое и информационное обеспечение фондов оценочных средств (см. карту литературного обеспечения дисциплины).

6. Оценочные средства (контрольно-измерительные материалы)
«Защита информации / Информационная безопасность»
по очной форме обучения

Учебные научно-исследовательские проекты (УНИП)

Тематика УНИП

1. Информационная безопасность современного общества.
2. Обзор нормативной документации РФ в сфере информационной безопасности.
3. Преступления в области информационной безопасности.
4. Феномен информационного права: опыт, проблемы, перспективы.
5. История методов и средств защиты информации.
6. Великие криптологи.
7. Информационная безопасность в современной предметной области «Информатика и ИТ».
8. Информационная безопасность в школьном курсе информатики и ИТ.
9. Современные средства защиты информации.
10. Технологии обеспечения информационной безопасности.
11. Современные стандарты шифров.
12. Тенденции развития криптографии (прикладной аспект).
13. Защита персональной информации на всех уровнях.
14. Безопасность современных операционных систем.
15. Информационная безопасность в сфере ИКТ.
16. Современные технические средства защиты информации.
17. Математические основы технологий защиты информации.
18. Информационная безопасность в системе профессионального образования РФ.

Темы проектов

Блок «История криптологии»

1. Аспекты формирования истории криптологии (какие существуют источники, кто первые авторы по данным темам, какая периодизация).
2. Криптология в Древнем мире (предпосылки, основные шифры и криптологи).
3. Криптология в эпоху Средневековья (предпосылки, основные шифры и криптологи).
4. Криптология в позднем Средневековье и в эпоху Возрождения (предпосылки, основные шифры и криптологи).
5. Криптология на предсовременном этапе (предпосылки, основные шифры и криптологи).
6. Криптология в России (предпосылки, основные шифры и криптологи).
7. Великие математики и криптология (рассмотреть либо 1-3 подробно в одном периоде, либо несколько на протяжении всей истории).

8. Великие кибернетики и криптология (рассмотреть либо 1-3 в одном периоде; либо несколько на протяжении всей истории, обязательно Алана Тьюринга, Клода Шеннона).
9. Начало компьютерной криптологии (первые компьютерные шифры и методы их взлома, криптологи-программисты).
10. Современное положение криптологии (области применения криптоалгоритмов, влияние на основные аспекты информационной безопасности).

Практические занятия

Практическая работа № 1-2.

Основные понятия ИБ.

Основа организации: групповая и индивидуальная работа
Форма представления результатов: отчет
Форма зачета: балл в рейтинге
Стоимость работы в рейтинге: 2+2 балла

Задание

(№ 1-5 выполняется в рабочих группах по 2-3 человека)

ФИО _____

Группа _____

1. Выпишите названия и краткое описание основных нормативных документов в области информационного права, результаты представьте в виде таблицы.

№	Документ (название, выходные данные)	Регулирует, предписывает	Ключевые понятия

2. Перечислите государственные органы РФ, контролирующие деятельность в области защиты информации

№	Название	Основные функции	Подчиненные структуры

3. Используя не менее, чем 5 различных источников дать определения следующим понятиям: 1) информационная безопасность; 2) уровни и составляющие информационной безопасности 3) защита информации; 4) компьютерная безопасность.
4. Прочитайте Стратегию развития информационного общества в Российской Федерации от 7 февраля 2008 г., определите и выпишите какие позиции данного документа связаны с вопросами информационной безопасности РФ.
5. Приведите и расшифруйте основные категории стандартной модели информационной безопасности.
6. Приведите основные составляющие информационной безопасности с точки зрения системного подхода, приведите их описания.
7. **Индивидуально** напишите развернутый ответ (7-8 предложений) на следующий вопрос: «Какова роль учителя информатики в вопросах становления информационного общества с точки зрения информационной безопасности?».
8. **Результаты вашей работы отправьте на адрес user@mailserver.com**

Практическая работа № 3-4.

Ценность информации и правовое регулирование вопросов ИБ.

Основа организации: групповая
Форма представления результатов: отчет
Форма зачета: балл в рейтинге
Стоимость работы в рейтинге: 2+2 балла

Задание

(выполняется в рабочих группах по 2 человека)

ФИО _____
Группа _____

I. Сохраните данный документ как «Отчет по лр № 2-3 (ЗИ) ФИО»

II. Ответьте на следующие вопросы:

9. В чем суть комплексного (системного) подхода к информационной безопасности? Приведите основные уровни (группы методов) обеспечения ИБ (обычно их выделяют четыре, иногда добавляют пятый – экономический).
10. Информацию правомочно рассматривать как товар, имеющий определенную цену. Цена, как и ценность информации, связана с полезностью информации для конкретных субъектов информационных отношений (личностей, организаций, сообществ, государств). Ценность информации субъективна, то есть сведения, важные и полезные для одних, совершенно нейтральны для других. Приведите пример, когда ценная информация не может быть товаром. Обоснуйте почему.
11. Измерение ценности информации – задача далеко не тривиальная. Метрические свойства информации представляют ее количественные характеристики, которые можно определить несколькими методами. Сформулируйте основные позиции (как измерять) для некоторых из них:
    - . Комбинаторный (Р.Хартли)
    - . Статистический (Энтропийный подход: К.Шеннон/А.Харкевич)
    - . Алгоритмический (А.Н. Колмогоров)
    - . Метрологический (Объем знаний, тезаурусный подход Ю.А. Шрейдера)
12. Что такое прагматические и семантические характеристики информации?
13. Назовите три категории ценности коммерческой информации.
14. Сформулируйте основные направления международного сотрудничества РФ в области ИБ.
15. Что содержится в международных документах касательно ИБ, имеющих условные названия: «Оранжевая книга», «Красная книга», «Зеленая книга», «Белая книга». Почему они были так названы?
16. Что такое международное право массовой информации? Как оно связано с вопросами ИБ? Какие международные организации наиболее активно принимают участие в формировании правовой базы информационной сферы?
17. Для чего нужна электронная цифровая подпись? Каким образом определяется юридическая сила электронного документа и электронной цифровой подписи в РФ?
18. Где и когда возник термин «компьютерная преступность»? Как менялось значение этого термина в праве? Как на сегодняшний день производится классификация компьютерных преступлений?
19. Кто такой хакер? Есть ли определение данного лица в информационном праве?
20. Какие два вида информации выделяются в информационном праве в качестве предмета преступления? Какие компьютерные преступления относятся к уголовно-наказуемым?

III. Результаты вашей работы отправьте на адрес user@mailserver.com

Практическая работа № 5-6

Контрольные вопросы и задания:

1. В чем заключается идея шифрования текста с помощью атбаша:

А) Замена символов одного алфавита символами другого

Б) Преобразование символа открытого текста в числовой код

В) Результирующий символ шифра – это симметричное отображение относительно «среднего»

Г) Результирующий символ – это символ, получаемый сдвигом по алфавиту на КЛЮЧ символов

2. Для чего нужны функции chr и ord?
3. Напишите фрагмент алгоритма расшифрования зашифрованного символа с помощью шифра Цезаря на языке Паскаль (обязательно укажите описание переменных).
4. Дан алфавит А={А, В, Н, О, Р }. Зашифруйте слово ВОРОНА с помощью Шифра Цезаря с ключом = 3.

Практическая работа № 7

Шифры эпохи Возрождения: таблица Вижинера и квадрат Бьюфорта.

1. Создайте в тетради или текстовом процессоре таблицу Вижинера размерностью 7×3 и алфавитом А={Н, А, Д, О, В, Р}. Зашифруйте слово ДВОР с помощью ключа ДНО.
2. С помощью этой же таблицы зашифруйте произвольное слово (не более 6 букв) с ключом РОВ. Напишите получившуюся шифрограмму на доске. Расшифруйте шифрограммы других студентов.
3. С помощью этой же таблицы зашифруйте произвольное слово (не более 6 букв) с произвольным ключом (не более 4 букв). Напишите получившуюся шифрограмму на доске. Расшифруйте шифрограммы других студентов. Какой метод для подбора ключа бы будете использовать?
4. Создайте в тетради или текстовом процессоре квадрат Бьюфорта размерностью 5×5 и алфавитом А={А, Е, О, П, Р}. Расшифруйте шифрограмму ЕААР с помощью ключа ПА.
5. С помощью этого же квадрата расшифруйте шифрограмму ЕАЕАПН, если известно, что размерность ключа от 3 до 6 символов.
6. Зашифруйте с помощью этого же квадрата произвольное слово не более чем из 5 символов и ключом ПЕРО с количеством раундов = 2. Запишите шифрограмму на доске. Расшифруйте шифрограммы других студентов.
7. Используя интерфейс, аналогичный программе «Квадрат Полибия» с помощью Delphi напишите программу шифрования текстовых файлов методом Вижинера или Бьюфорта.

Итоговая контрольная работа.

1. Что понимается под информационной безопасностью:

A. защита душевного здоровья телезрителей

B. защита от нанесения неприемлемого ущерба субъектам информационных отношений

X. обеспечение информационной независимости России

2. Что из перечисленного не относится к числу основных аспектов информационной безопасности:

A. Доступность
B. Масштабируемость
C. Целостность
D. Конфиденциальность

3. Что из перечисленного относится к числу основных аспектов информационной безопасности:

A. подлинность - аутентичность субъектов и объектов

B. целостность - актуальность и непротиворечивость информации, защищенность информации и поддерживающей инфраструктуры от разрушения и несанкционированного изменения

C. стерильность - отсутствие недекларированных возможностей

4. Сложность обеспечения информационной безопасности является следствием:

A. комплексного характера данной проблемы, требующей для своего решения привлечения специалистов разного профиля
B. наличия многочисленных высококвалифицированных злоумышленников
C. развития глобальных сетей

5. Уголовный кодекс РФ не предусматривает наказания за:

A. увлечение компьютерными играми в рабочее время
B. неправомерный доступ к компьютерной информации
C. нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

6. Согласно Закону "Об информации, информатизации и защите информации", риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на:

A. владельце этой системы
B. собственнике документов
C. потребителе информации

7. Действие Закона "О лицензировании отдельных видов деятельности" не распространяется на:

1. деятельность по технической защите конфиденциальной информации
2. образовательную деятельность в области защиты информации
3. предоставление услуг в области шифрования информации

8. В следующих странах сохранилось жесткое государственное регулирование разработки и распространения криптосредств на внутреннем рынке:

5. Китай
6. Россия
7. Франция

9. Под определение средств защиты информации, данное в Законе "О государственной тайне", подпадают:

A. средства выявления злоумышленной активности
B. средства обеспечения отказоустойчивости
C. средства контроля эффективности защиты информации

10. Закон "Об информации, информатизации и защите информации" на первое место ставит:

A. сохранение конфиденциальности информации
B. поддержание целостности информации
C. обеспечение доступности информационных услуг

11. Криптология – это _____.

12. Основные разделы криптологии:

1)_____, которая занимается вопросами_____.
2)_____, которая занимается вопросами_____.
3)_____, который занимается вопросами_____.

13. Шифр – это _____.

14. Открытый текст (plain text) – это _____.

14. Ключ шифра – это _____.

15. Код и шифр понятия тождественные да/нет, потому что _____.

16.Тайнопись отличается от криптографии с ключом тем, что _____.

17. В зависимости от используемых ключей шифрования и расшифрования криптоалгоритмы подразделяются на две группы: _____.

18. По характеру воздействий, производимых над данными криптоалгоритмы подразделяются на _____.

19. По величине блока данных криптоалгоритмы подразделяются на ____.

20. Историю криптологии условно разделяют на два периода:

A. «дописьменный» и «письменный»
B. «ручной» и «машинный»
C. «математический» и «кибернетический»
D. «донаучный» и «научный»

21. Автором первого фундаментального труда в области криптологии на современном этапе является

A. Д. Кан
B. В. Жельников
C. А. Бабаш
D. Ф. Смит

22. К отечественным ученым-криптологам современного этапа не относится

A. В. Жельников
B. А. Бабаш
C. Т. Соболева
D. В. Крестовский

23. Первые способы защиты информации появились в связи с

A. Началом войн
B. Возникновением первых государств
C. Обособлением племен
D. Возникновением письменности

24. Основной недостаток стеганографии (тайнописи) по сравнению с криптографией заключается в

A. Сравнительно недолгой эффективности стеганографии в связи с прогрессом науки и техники
B. Том, что защита информации при помощи стеганографии требует больших материальных затрат
C. Относительной открытости всех методов
D. Трудоемкости извлечения исходного сообщения

25. Понятие кода считается _____к понятию шифра

A. Тождественным
B. Противоположным
C. Абсолютно не связанным
D. Дополняющим

26. Упадок криптологии в Средние века в Европе связывают с

Общим упадком культуры и науки
Обособлением отдельных государств
Периодом прекращения войн
Появлением правовых государств

27. Христианская церковь относилась к криптологии в Средние века:

Всячески поддерживала исследования, в том числе и монахов
Никаким образом не влияла
Преследовала ученых, считала колдовством и ересью
Не одобряла, однако не преследовала ученых

28. Состояние криптологии в арабском мире в Средние века

A. Резко пришло в упадок
B. Стремительно улучшилось и потом пошло на спад
C. Оставалось на уровне античности
D. Ухудшалось из-за преследований мусульманской церкви

29. Автором труда «О большом стремлении человека разгадать загадки древней письменности» является

A. Г. Галилей
B. Шебах Калкандаши
X. Абу-Бакра Набати
Δ. Август II

30. Идея криптоанализа Калкандаши состоит в использовании

A. Специальных решеток
B. Символов из европейских алфавитов
C. Статистических данных
D. Полного перебора вариантов замены

31. В чем заключается идея шифрования текста с помощью атбаша:

A. Замена символов одного алфавита символами другого
B. Преобразование символа открытого текста в числовой код
C. Результирующий символ шифра – это симметричное отображение относительно «среднего»
D. Результирующий символ – это символ, получаемый сдвигом по алфавиту на КЛЮЧ символов

32. Для чего нужны функции chr и ord в Delphi?
Chr-_____
Ord-_____

33. Дан алфавит A={A, B, H, O, P }. Зашифруйте слово ВОРОНА с помощью Шифра Цезаря с ключом = 3.

_____

34. В чем заключается идея шифрования текста с помощью квадрата Бьюфорта:

1. Использование числовых последовательностей
2. Преобразование кода происходит с помощью систем уравнений
3. Используется прямоугольная таблица с определенным расположением символов
4. Преобразование символа открытого текста в числовой код и обратно происходит посредством символов другого алфавита.

35. Зашифруйте слово МАНА с помощью шифра Полибия с параметрами: 2×2, ключ 11, алфавит: {Н, А, М, пробел}.

36. При скремблировании любой файл рассматривается как последовательность _____ и используются операции _____,__ ____,_____,_____.

Перечень вопросов к зачету

1. Понятие информационной безопасности, основные определения.
2. Основные составляющие информационной безопасности.
3. Категории информационной безопасности.
4. Абстрактные модели защиты информации.
5. Сервисы безопасности.
6. Законодательный уровень информационной безопасности.
7. Феномен информационного права.
8. Обзор российского законодательства в области информационной безопасности.
9. Преступления в сфере защиты информации.
10. Шифрование и криптография: базовая терминология.
11. Классификация криптоалгоритмов.
12. Стойкость алгоритмов шифрования.
13. Области применения криптоалгоритмов.
14. Криптология в Древнем мире.
15. Криптология в Средние века.
16. Криптология в позднее средневековье и эпоху Возрождения.
17. Криптология на предсовременном этапе(XVIII–начало XX вв.).
18. Криптография и криптоанализ в России.
19. Современное положение криптологии.
20. Симметричные криптоалгоритмы.
21. Простейшие методы шифрования текста.
22. Классификации криптоалгоритмов.
23. Посимвольное шифрование текста: замены и перестановки.
24. Поточное шифрование. Скремблеры.
25. Блочные шифры. Стандарт AES. Шифр TEA.

26. Асимметричные криптоалгоритмы. Шифр RSA.
27. Российские криптосистемы.
28. Цифровая подпись.
29. Пароли и хеширование.
30. Криптоанализ. Области применения и основные методы.
31. Технологии защиты персональных данных.
32. Информационная безопасность предприятий.
33. Прикладные средства обеспечения информационной безопасности.
34. Вредоносное ПО: история, классификация, особенности.
35. Методы защиты от вредоносного ПО.
36. Безопасность современных сетевых технологий.
37. Методы комплексного обеспечения компьютерной безопасности.
38. Информационная безопасность в предметной области «Информатика и ИТ».

Карта литературного обеспечения дисциплины

ЗАЩИТА ИНФОРМАЦИИ / ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление 44.03.05 «Педагогическое образование»

Профиль: «Математика и информатика»

Квалификация: бакалавр

Очная форма обучения

(общая трудоемкость 2,0 з.е.)

Наименование	Наличие место/ (кол-во экз.)	Потребность	Примечания
Обязательная литература			
Входной модуль			
Прохоров, А. А. Основы информатики и вычислительной техники в 5 ч.: учебное пособие. Части 1-5. - Красноярск: КГПУ им. В. П. Астафьева, 2007-2011.	50	35	Метод кабинет
Могилев, А.В. Практикум по информатике: Учеб. пособие для студ. высш. учеб. заведений/ А.В. Могилев, Н.И. Пак Н.И., Е.К. Хеннер; Ред. Е.К. Хеннер. - М.: "Академия", 2002. - 608 с.	66	35	ОБИМФИ
Бен-Ари, М. Языки программирования. Практический сравнительный анализ: Пер. с англ/ М. Бен-Ари. - М.: Мир, 2000. – 366 с.	1	35	ОБИМФИ
Гордеев, А.В.Системное программное обеспечение: учебник для вузов/ А.В. Гордеев, А.Ю. Молчанов. - СПб.: Питер, 2003. - 736 с.	3	10	ОБИМФИ
Модуль №1-3			
Хорев, П.Б.Методы и средства защиты информации в компьютерных системах: Учебное пособие для студ. высш. учеб. заведений/ П.Б. Хорев. - М.: Академия, 2005. - 256 с.	17	15	ОБИМФИ
Мельников, В.П. Информационная безопасность: Учебное пособие для сред. проф. образования/ В.П. Мельников, С.А. Клейменов, А.М. Петраков; Ред. С.А. Клейменов. - М.: Академия, 2005. - 336 с.	18	15	ОБИМФИ
Куприянов, А.И. Основы защиты информации: Учебное пособие для студ. высш. учеб. заведений/ А.И. Куприянов. - М.: Академия, 2006. - 256 с.	47	35	ОБИМФИ
Ломаско, П.С. Информационная безопасность: теория, практика, жизнь. Учебное пособие для студ. высш. пед. учеб. заведений/ П.С. Ломаско. - Красноярск: КГПУ им. В. П. Астафьева, 2012. - 250 с.	1	35	Электронный ресурс
Дополнительная литература			
Модули 1-3			
Зегжда, Д.П. Основы безопасности информационных систем: учебное пособие/ Д.П. Зегжда, А.М. Ивашко. - М.: Горячая линия - Телеком, 2000. - 452 с.	4	5	ОБИМФИ
Одинцов, А. А. Защита предпринимательства (Экономическая и информационная безопасность). Учеб. пособие/ А. А. Одинцов. - М.: Международные отношения, 2003.	8	5	ОБИМФИ
Галатенко, В.А. Основы информационной безопасности: Курс лекций. Учебное пособие/ В.А.	10	5	ОБИМФИ

Галатенко. Под ред. В.Б. Бетелина. - 2-е изд., испр. . - М.: ИНТУИТ.РУ, 2009. - 264 с.			
Основы научных исследований: теория и практика: Учеб. пособие для студ. вузов, обуч. по спец. в области информ. безопасности/ В.А. Тихонов и др.. - М.: Гелиос, 2006. - 352 с.	5	5	ОБИМФИ
Основы компьютерных сетей: Учебное пособие. - М.: Бином. Лаборатория Знаний, 2006. - 167 с.: ил.	4	4	ОБИМФИ
Элективный курс "Основы информационной безопасности при работе в телекоммуникационных сетях": методическое пособие/ И. А. Калинин, Н. Н. Самылкина. - М.: Чистые пруды, 2007. - 32 с.	2	2	ОБИМФИ

КАРТА МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ / ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление 44.03.05 «Педагогическое образование»

Профиль: «Математика и информатика»

Квалификация: бакалавр

Очная форма обучения

(общая трудоемкость 2,0 з.е.)

Аудитория	**Оборудование**
Лекционные аудитории	
Ул. Перенсона ,7. ауд. № 3-02	ПК с ОС Windows, проектор мультимедиа, интерактивная доска SMART-board. маркерная доска
Ул. Перенсона ,7. ауд. № 2-04	ПК с ОС Windows, проектор мультимедиа, интерактивная доска SMART-board. маркерная доска
Аудитории для практических (семинарских)/ лабораторных занятий	
Ул. Перенсона ,7. ауд. 2-04	10 ПК с ОС Windows + MS Office, проектор мультимедиа, интерактивная доска SMART-board. маркерная доска

Лист внесения изменений

Дополнения и изменения в учебной программе на 2016/2017 учебный год нет.

Рабочая программа утверждена на заседании базовой кафедры информатики и ИТ в образовании "05"октября 2016 г. (протокол заседания кафедры № 03)

Заведующий кафедрой _____ Пак Н.И.

Директор _____ Чиганов А.С.