Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Комсомольский-на-Амуре государственный университет»

Кафедра «Информационная безопасность автоматизированных систем»

УТВЕРЖДАЮ
Первый проректор
_____ И.В. Макурин
«__» 02 _____ 2018 г.

8 ДАБ-1/108

РАБОЧАЯ ПРОГРАММА
дисциплины «Введение в криптографию» основной образовательной программы подготовки бакалавров по направлению 46.03.02 **«Документоведение и архивоведение** профиль «Историко-архивоведение»

Форма обучения очная
Технология обучения традиционная

Комсомольск-на-Амуре 2018 г.

Автор рабочей программы д.т.н. _____ В. А. Челухин
профессор кафедры «Информационная безопасность автоматизированных систем», «30» 01 2018 г.

СОГЛАСОВАНО

Директор библиотеки _____ И.А. Романовская
«06» 02 2018 г.

Заведующий кафедрой _____ Ж. В. Петрунина
«История и архивоведение» «01» 02 2018 г.

Декан СГФ
_____ И.В. Цевелева
«05» 02 2018 г

Начальник учебно-методического управления _____ Е .Е. Поздеева
"08" 02 2018 г.

Введение

Рабочая программа дисциплины «Введение в криптографию» составлена в соответствии с требованиями федерального государственного образовательного стандарта, утвержденного приказом Министерства образования и науки Российской от 06.03.2015 N 176 "Об утверждении федерального государственного образовательного стандарта высшего образования по направлению подготовки 46.03.02 Документоведение и архивоведение (уровень бакалавриата)" и образовательной программы подготовки бакалавров **«Документоведение и архивоведение»** профиль 46.03.02 «Историко-архивоведение».

1 Аннотация дисциплины

<table>
<tr><td>Наименование дисциплины</td><td colspan="7">Введение в криптографию</td></tr>
<tr><td>Цель дисциплины</td><td colspan="7">Ознакомить студентов с основами криптографии и сформировать достаточно глубокие знания о:
- Основных понятиях криптографии;
- Основных задачах криптографии;
- Математических основ криптографии</td></tr>
<tr><td>Задачи дисциплины</td><td colspan="7">• изучение теоретических принципов криптографии;
• изучение истории криптографии
• развитие аналитического мышления студентов и повышение их общей математической культуры.</td></tr>
<tr><td>Основные разделы дисциплины</td><td colspan="7">История и основы криптографии
Симметричная криптография
Криптография с открытым ключом.</td></tr>
<tr><td rowspan="3">Общая трудоемкость дисциплины</td><td colspan="7">3 з.е. / 108 академических часов</td></tr>
<tr><td rowspan="2">Семестр</td><td colspan="3">Аудиторная нагрузка, ч</td><td rowspan="2">СРС, ч</td><td rowspan="2">Промежуточная аттестация, ч</td><td rowspan="2">Всего за семестр, ч</td></tr>
<tr><td>Лекции</td><td>Пр. занятия</td><td>контроль</td></tr>
<tr><td>5 семестр</td><td>16</td><td>16</td><td></td><td>76</td><td></td><td>108</td></tr>
<tr><td colspan="2">ИТОГО:</td><td>16</td><td>16</td><td></td><td>76</td><td></td><td>108</td></tr>
</table>

2 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Дисциплина «Введение в криптографию» нацелена на формирование компетенций, знаний, умений и навыков, указанных в таблице 1.

Таблица 1 – Компетенции, знания, умения, навыки

Наименование и шифр компетенции, в формировании которой принимает участие дисциплина	Перечень формируемых знаний, умений, навыков, предусмотренных образовательной программой		
	Перечень знаний (с указанием шифра)	Перечень умений (с указанием шифра)	Перечень навыков (с указанием шифра)
ОПК-1 способностью использовать теоретические знания и методы исследования на практике	З1(ОПК-1-2) виды информационных угроз;	У1(ОПК-1-2) применять алгоритмы криптографии для защиты информации	Н1(ОПК-1-2) современными методами криптографической защиты информации

3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Введение в криптографию» изучается на 3 курсе в 5 семестре. Дисциплина входит в состав блока «Дисциплины (модули)» базовой части.

Для освоения дисциплины необходимы знания, умения и навыки, формируемые в процессе изучения дисциплины «Информатика».

4 Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 3 зачетных единиц, 108 академических часов.

Распределение объема дисциплины (модуля) по видам учебных занятий представлено в таблице 2.

Таблица 2 – Объем дисциплины (модуля) по видам учебных занятий

Объем дисциплины	**Всего академических часов**
	Очная форма обучения
	16 недель в семестре
Общая трудоемкость дисциплины	108
Контактная аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего	32
В том числе:	

Объем дисциплины	Всего академических часов
	Очная форма обучения
	16 недель в семестре
занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками)	16
занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия)	16
Самостоятельная работа обучающихся и контактная работа, включающая групповые консультации, индивидуальную работу обучающихся с преподавателями (в том числе индивидуальные консультации); взаимодействие в электронной информационно-образовательной среде вуза	76
Промежуточная аттестация обучающихся	

5 Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Таблица 3 – Структура и содержание дисциплины (модуля)

Наименование разделов, тем и содержание материала	Компонент учебного плана	Трудоёмкость, ч	Форма проведения	Планируемые (контролируемые) результаты освоения	
				Компетенции	Знания, умения, навыки
Раздел 1 История и основы криптографии					
Основные понятия и определения криптографии	Лекция	1	Интерактивная (презентация)	ОПК-1	З1(ОПК-1-1)
История криптографии	Лекция	2	Интерактивная (презентация)	ОПК-1	З1(ОПК-1-1)
Криптоанализ исторических шифров	Лекция	2	Интерактивная (презентация)	ОПК-1	З1(ОПК-1-1)
Криптоанализ исторических шифров	Практические занятия	2	Традиционная	ОПК-1	З1(ОПК-1-1)
Криптографическая стойкость	Лекция	2	Интерактивная (презентация)	ОПК-1	З1(ОПК-1-1)

Наименование разделов, тем и содержание материала	Компонент учебного плана	Трудоёмкость, ч	Форма проведения	Планируемые (контролируемые) результаты освоения	
				Компетенции	Знания, умения, навыки
Криптографическая стойкость	Практические занятия	2	Традиционная	ОПК-1	У1(ОПК-1-1)
Раздел 2 Симметричная криптография					
Поточные шифры	Лекция	1	Традиционная	ОПК-1	З1(ОПК-1-1)
Поточные шифры	Практические занятия	2	Традиционная	ОПК-1	Н1(ОПК-1-1)
Блочные шифры	Лекция	1	Традиционная	ОПК-1	З1(ОПК-1-1)
Блочные шифры	Практические занятия	2	Традиционная	ОПК-1	Н1(ОПК-1-1)
Алгоритм шифрования DES и его модификации	Лекция	1	Традиционная	ОПК-1	З2(ОПК-1-1)
Алгоритм шифрования DES и его модификации	Практические занятия	2	Традиционная	ОПК-1	У1(ОПК-1-1)
Режимы работы блочных шифров	Лекция	1	Традиционная	ОПК-1	З2(ОПК-1-1)
Режимы работы блочных шифров	Практические занятия	2	Интерактивная	ОПК-1	У1(ОПК-1-1)
Advanced encryption standard	Лекция	1	Традиционная	ОПК-1	З2(ОПК-1-1)
Раздел 3 Криптография с открытым ключом					
Целостность и аутентификация сообщений	Лекция	1	Традиционная	ОПК-1	З2(ОПК-1-1)
Целостность и аутентификация сообщений	Практические занятия	2	Интерактивная	ОПК-1	У1(ОПК-1-1)
Основы теории чисел	Лекция	1	Традиционная	ОПК-1	З2(ОПК-1-1)
Криптография с открытым ключом	Лекция	1	Традиционная	ОПК-1	З2(ОПК-1-1)
Криптография с открытым ключом	Практические занятия	2	Традиционная	ОПК-1	Н2(ОПК-1-1)
Аутентификация и электронно-цифровая подпись	Лекция	1	Традиционная	ОПК-1	З2(ОПК-1-1)
	Самостоятельная работа обучающихся (подго-	30	Освоение электронных материалов по дисциплине.	ОПК-1	У1(ОПК-1-1)

Наименование разделов, тем и содержание материала	Компонент учебного плана	Трудоёмкость, ч	Форма проведения	Планируемые (контролируемые) результаты освоения	
				Компетенции	Знания, умения, навыки
	товка к практическим занятиям)				
	Самостоятельная работа обучающихся (изучение теоретических разделов дисциплины)	30	Чтение основной и дополнительной литературы, конспектирование	ОПК-1	З2(ОПК-1-1)
	Самостоятельная работа обучающихся (подготовка контрольной работы)	26	Подбор литературы. Выполнение расчетов.	ОПК-1	У2(ОПК-1-1)
ИТОГО по дисциплине	Лекции	16	-	-	-
	Практические работы	16		-	-
	Самостоятельная работа обучающихся	76	-	-	-
	контроль				
ИТОГО: общая трудоемкость дисциплины 108 часов					

6 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа обучающихся, осваивающих дисциплину «Введение в криптографию», состоит из следующих компонентов: подготовка к лекциям и практическим занятиям, решение и оформление контрольной работы.

Для успешного выполнения всех разделов самостоятельной работы учащимся рекомендуется использовать следующее учебно-методическое обеспечение:

1. Введение в криптографию: Учебное пособие / Ященко В.В., - 4-е изд. - М.:МЦНМО, 2014. - 352 с // ZNANIUM.COM.: электронно-библиотечная система. – Режим доступа: http://znanium.com/catalog/product/958585, ограниченный. – Загл. с экрана.

Рекомендуемый график выполнения самостоятельной работы представлен в таблице 4.

таблица 4.

Виды самостоятельной работы	Число часов в неделю																Итого по видам работ
Недели	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
подготовка к практическим занятиям	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	1	30
изучение теоретических разделов дисциплины	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	1	30
подготовка контрольной работы			2	2	2	2	2	2	2	2	2	2	2	2	2		26
Итого	4	4	6	6	6	6	6	6	6	6	6	6	6	6	4	2	76

Общие рекомендации по организации самостоятельной работы.

Время, которым располагает студент для выполнения учебного плана, складывается из двух составляющих: одна из них – это аудиторная работа в вузе по расписанию занятия, другая – внеаудиторная самостоятельная работа. Задания и материалы для самостоятельной работы выдаются во время учебных занятий по расписанию, на этих же занятиях преподаватель осуществляет контроль за самостоятельной работой, а также оказывает помощь студентам по правильной организации работы.

Чтобы выполнить весь объем самостоятельной работы, необходимо заниматься по 1 – 3 часа ежедневно. Начинать самостоятельные внеаудиторные занятия следует с первых же дней семестра. Первые дни семестра очень важны для того, чтобы включиться в работу, установить определенный порядок, равномерный ритм на весь семестр. Ритм в работе – это ежедневные самостоятельные занятия, желательно в одни и те же часы, при целесообразном чередовании занятий с перерывами для отдыха.

Начиная работу, не нужно стремиться делать вначале самую тяжелую ее часть, надо выбрать что-нибудь среднее по трудности, затем перейти к более трудной работе. И напоследок оставить легкую часть, требующую не сколько больших интеллектуальных усилий, сколько определенных действий (построение графиков и т.п.).

Следует правильно организовать свои занятия по времени: 50 минут – работа, 5-10 минут – перерыв; после 3 часов работы перерыв – 20-25 минут. Иначе нарастающее утомление повлечет неустойчивость внимания. Очень существенным фактором, являются систематические занятия физической культурой. Организация активного отдыха предусматривает чередование умственной и физической деятельности, что полностью восстанавливает работоспособность человека

7 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Таблица 5 – Паспорт фонда оценочных средств

Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства	Показатели оценки
1. История и основы криптографии	ОПК-1	Практическое задание теме № 1	Знает историю развития криптографии и понимает основы криптографии
2. Симметричная криптография	ОПК-1	Практическое задание теме № 2	Знает и умеет использовать симметричную криптографию.
3. Криптография с открытым ключом	ОПК-1	Практическое задание теме № 3	Показать знания и умения по первым двум темам
Темы 1, 2, 3	ОПК-1	Контрольная работа	Знает и умеет использовать криптографию с открытым ключом

Промежуточная аттестация проводится в форме зачета. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, представлены в виде технологической карты дисциплины (таблица 6).

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
4семестр ***Промежуточная аттестация в форме зачета***				
1	Практическое задание по заданной теме № 1	В течение семестра	5 баллов	5 баллов - студент правильно выполнил задание. Показал отличные знания в рамках освоенного учебного материала. 4 балла - студент выполнил задание, с небольшими неточностями. Показал хорошие знания в рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания в рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
2	Практическое задание по заданной теме № 2	В течение семестра	5 баллов	5 баллов - студент правильно выполнил задание. Показал отличные знания в рамках освоенного учебного материала. 4 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания в рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания в рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено.
3	контрольная работа	В течение семестра	15 баллов	15 баллов - студент правильно выполнил рефераты. Показал отличные владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала.. 10 баллов - студент выполнил рефераты с небольшими неточностями. Показал хорошие владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. 5 баллов - студент выполнил рефераты с существенными неточностями. Показал удовлетворительное владение навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала. 0 баллов - при выполнении задания студент продемонстрировал недостаточный уровень владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного учебного материала.

	Наименование оценочного средства	Сроки выполнения	Шкала оценивания	Критерии оценивания
4	Практическое задание по заданной теме № 3	В течение семестра	10 баллов	10 баллов - студент правильно выполнил задание. Показал отличные знания в рамках освоенного учебного материала. 5 балла - студент выполнил задание с небольшими неточностями. Показал хорошие знания в рамках освоенного учебного материала. 3 балла - студент выполнил задание с существенными неточностями. Показал удовлетворительные знания в рамках освоенного учебного материала. 2 балла - при выполнении задания студент продемонстрировал недостаточный уровень знаний. 0 баллов – задание не выполнено
4				
ИТОГО:			**35 баллов**	

Критерии оценки результатов обучения по дисциплине:

Максимальный балл текущего контроля составляет 35 баллов;

Максимальный итоговый рейтинг – 35 баллов.

Оценке «зачтено» соответствует 20-35 баллов;

Менее 15 «не зачтено»

Задания для текущего контроля

Практическое задание 1 – Сгенерировать 2 байта псевдослучайной последовательности, генерируемой регистром сдвига с линейными обратными связями в соответствии со своим вариантом. Начальное заполнение выбрать случайным.

№ варианта	Образующий многочлен	Схема регистра
1	$\Phi(x) = x^{19} \oplus x^5 \oplus x^2 \oplus x \oplus 1$	Галуа
2	$\Phi(x) = x^{18} \oplus x^7 \oplus 1$	Фибоначчи
3	$\Phi(x) = x^{13} \oplus x^4 \oplus x^3 \oplus x \oplus 1$	Галуа
4	$\Phi(x) = x^{17} \oplus x^3 \oplus 1$	Фибоначчи
5	$\Phi(x) = x^{13} \oplus x^4 \oplus x^3 \oplus x \oplus 1$	Фибоначчи
6	$\Phi(x) = x^{16} \oplus x^{12} \oplus x^3 \oplus x \oplus 1.$	Галуа
7	$\Phi(x) = x^{15} \oplus x \oplus 1.$	Фибоначчи
8	$\Phi(x) = x^{16} \oplus x^{12} \oplus x^3 \oplus x \oplus 1.$	Фибоначчи
9	$\Phi(x) = x^{18} \oplus x^7 \oplus 1$	Галуа
10	$\Phi(x) = x^{17} \oplus x^3 \oplus 1$	Галуа
11	$\Phi(x) = x^{14} \oplus x^{10} \oplus x^6 \oplus x \oplus 1$	Фибоначчи
12	$\Phi(x) = x^{12} \oplus x^6 \oplus x^4 \oplus x \oplus 1$	Галуа
13	$\Phi(x) = x^{12} \oplus x^6 \oplus x^4 \oplus x \oplus 1$	Фибоначчи
14	$\Phi(x) = x^{15} \oplus x \oplus 1.$	Галуа
15	$\Phi(x) = x^{19} \oplus x^5 \oplus x^2 \oplus x \oplus 1$	Фибоначчи

Практическое задание 2 – Необходимо найти число $a^n mod\ p$. Использовать алгоритм быстрого возведения в степень

Номер варианта	a	n	p
1	11	112	17
2	7	126	11
3	13	108	17
4	8	120	13
5	9	115	11
6	12	119	13
7	8	129	11
8	9	131	13
9	8	117	13
10	8	109	11
11	11	122	9
12	9	118	7
13	13	105	9
14	9	123	11

15	7	127	7
16	2	133	9

Практическое задание 3 – Зашифровать шифром rot свою фамилию (номер варианта совпадает с номером в списке группы и является смещение в таблице).

Задания для контрольной работы

Задание 1 – Даны два числа a, b. Найти из наибольший общий делитель с помощью алгоритма Эвклида.

Номер варианта	a	b
1	172	185
2	198	136
3	201	187
4	145	200
5	196	178
6	205	179
7	190	167
8	214	167
9	197	186
10	158	202
11	157	182
12	177	174
13	163	194
14	173	175
15	189	162
16	212	169

Задание 2 – Дано число n. Требуется найти $\varphi(n)$. Использовать определение и свойства функции Эйлера

Номер варианта	n
1	66
2	65
3	44
4	45
5	60
6	48
7	62
8	51
9	56
10	57

11	58
12	52
13	46
14	64
15	42
16	40

Задания выполнить в соответствии с требованиями единой системы документации (ЕСПД) и РД 013-2016 «Текстовые студенческие работы. Правила оформления».

Структурными элементами данной работы должны быть:

- титульный лист;
- текст задания (в соответствии с вариантом);
- содержание;
- введение
- основная часть;
- заключение и выводы;
- список использованных источников;
- приложения.

Во введении дается краткое описание изучаемой дисциплины, которой посвящена данная работа, а также приводится обзор выполненной работы.

8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

8.1 Основная литература

1 Введение в криптографию: Учебное пособие / Ященко В.В., - 4-е изд. - М.:МЦНМО, 2014. – 352 с // ZNANIUM.COM.: электронно-библиотечная система. – Режим доступа: http://znanium.com/catalog/product/958585, ограниченный. – Загл. с экрана.

2 Просто криптография: Научно-популярное / Де Касто В. - Спб.:Страта, 2014. – 204 с. // ZNANIUM.COM.: электронно-библиотечная система. – Режим доступа: http://znanium.com/catalog/product/510235, ограниченный. – Загл. с экрана.

3 Кукина Е.Г. Введение в криптографию [Электронный ресурс] : сборник задач и упражнений / Е.Г. Кукина, В.А. Романьков. — Электрон. текстовые данные. — Омск: Омский государственный университет им. Ф.М. Достоевского, 2013. — 91 с. // IPRbooks: электронно-библиотечная система. – Режим доступа: http://www.iprbookshop.ru/24876.html, ограниченный. – Загл. с экрана.

4 Торстейнсон П. Криптография и безопасность в технологии .NET / Торстейнсон П., Ганеш Г.А.. — Москва : Лаборатория знаний, 2020. — 480 с.

— ISBN 978-5-00101-700-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/20709.html (дата обращения: 22.10.2021). — Режим доступа: для авторизир. Пользователей

5 Информационный мир XXI века. Криптография – основа информационной безопасности / Б.П. Елисеев [и др.].. — Москва : Дашков и К, Московский государственный технический университет гражданской авиации, 2019. — 126 c. — ISBN 978-5-394-03397-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/85368.html (дата обращения: 22.10.2021). — Режим доступа: для авторизир. пользователей

8.2 Дополнительная литература

1 Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов. - М.: Гор. линия-Телеком, 2010. - 232 с.: 60x90 1/16. (переплет) ISBN 978-5-9912-0150-6, ZNANIUM.COM.: электронно-библиотечная система. - Режим доступа: http://znanium.com/catalog/product/265565, ограниченный. – Загл. с экрана.

2 Кнауб, Л. В. Теоретико-численные методы в криптографии [Электронный ресурс] : Учеб. пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. - Красноярск : Сибирский федеральный университет, 2011. - 160 с. - ISBN 978-5-7638-2113-7. ZNANIUM.COM.: электронно-библиотечная система. - Режим доступа: http://znanium.com/catalog/product/441493, ограниченный. – Загл. с экрана.

3 Лекции по криптографии: Курс лекций / Музыкантский А.И., Фурин В.В., - 2-е изд., стереотип. - М.:МЦНМО, 2014. - 68 с.: ISBN 978-5-4439-2075-7 - ZNANIUM.COM.: электронно-библиотечная система.Режим доступа: http://znanium.com/catalog/product/958677, ограниченный. – Загл. с экрана.

4 Басалова Г.В. Основы криптографии : учебное пособие / Басалова Г.В.. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 282 c. — ISBN 978-5-4497-0340-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/89455.html (дата обращения: 22.10.2021). — Режим доступа: для авторизир. пользователей

9 Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), необходимых для освоения дисциплины (модуля)

1 Основы криптографии. // Национальный открытый университет «Интуит» [Электронный ресурс] – Режим доступа: https://www.intuit.ru/studies/courses/691/547/info - свободный.

10 Методические указания для обучающихся по освоению дисциплины (модуля)

Обучение дисциплине «Введение в криптографию» предполагает изучение курса на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проводятся в форме лекций и практических занятий.

Таблица 7 Методические указания к отдельным видам деятельности

Вид учебного занятия	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения. Выделять ключевые слова, формулы, отмечать на полях уточняющие вопросы по теме занятия
Практическое занятие	Работа с специальным программным обеспечением.
Самостоятельная работа	Для более глубокого изучения разделов дисциплины предусмотрены отдельные виды самостоятельной работы: подготовка к практическим занятиям, изучение теоретических разделов дисциплины, подготовка контрольной работы.

Самостоятельная работа является наиболее продуктивной формой образовательной и познавательной деятельности студента в период обучения. СРС направлена на углубление и закрепление знаний студента, развитие практических умений. СРС по дисциплине «Введение в криптографию» включает следующие виды работ:

– работу с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуальному заданию;

– опережающую самостоятельную работу;

– изучение тем, вынесенных на самостоятельную проработку;

– подготовку к практическим занятиям;

– выполнение и оформление контрольной работы.

Контроль самостоятельной работы студентов и качество освоения дисциплины осуществляется посредством:

– представления в указанные контрольные сроки результатов выполнения заданий для текущего контроля;

– выполнения контрольной работы.

– зачета.

Текущий контроль качества освоения отдельных тем дисциплины осуществляется на основе рейтинговой системы. Этот контроль осуществляется в течение семестра и качество усвоения материала (выполнения задания) оценивается в баллах, в соответствии с таблицей 6.

11 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

и информационных справочных систем (при необходимости)

1. Текстовый редактор MS Word 2010/2013.
2. Операционная система Windows 7, 8, 8.1, 10
3. MS SQL serverDreamspark (договор № Tr018039/M18 от 28.03.2013)
4. MS AccessDreamspark (договор № Tr018039/M18 от 28.03.2013)
5. Операционная система Windows 7, 8Dreamspark (договор № Tr018039/M18 от 28.03.2013)

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

Для реализации программы дисциплины «Введение в криптографию» используется материально-техническое обеспечение, перечисленное в таблице 8.

Таблица 8 – Материально-техническое обеспечение дисциплины

Аудитория	Наименование аудитории (лаборатории)	Используемое оборудование	Назначение оборудования
201/5	Лаборатория программно-аппаратных средств защиты информации	Восемь ноутбуков Lenovo B500, проектор + экран для демонстрации.	Для проведения видео лекций, работы со специальными программами, проектными работами.

Лист регистрации изменений к РПД

	Номер протокола заседания кафедры, дата утверждения изменения	Количество страниц изменения	Подпись разработчика РПД
1	Протокол заседания кафедры ИБАС № 2 от 12.10.2021	8	