Министерство сельского хозяйства Российской Федерации
Департамент образования и кадровой политики
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Красноярский государственный аграрный университет»

Центр подготовки специалистов среднего звена
Кафедра информационных технологий и математического обеспечения информационных систем

СОГЛАСОВАНО:
Директор ЦПССЗ
ТюринаЛ.Е.
« 24» февраля 2026 г.

УТВЕРЖДАЮ:
Ректор
Пыжикова Н.И.
«27» февраля 2026 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»
ФГОС СПО

по специальности 09.02.11 Разработка и управление программным обеспечением

Курс 2
Семестр 3
Форма обучения очная
Квалификация выпускника: программист
Срок освоения ОПОП 3г. 10м.

Красноярск, 2026

Составители: Романова Дарья Сергеевна, преподаватель

« 2 » февраля 2026 г.

Программа разработана в соответствии с ФГОС СПО по специальности 09.02.11 Разработка и управление программным обеспечением (№ 138 от 24.02.2025) и примерной основной образовательной программой (№ 01-09-581/2025 от 13.10.2025)

Программа обсуждена на заседании кафедры протокол № 6 «10» 02 2026 г.

Зав. кафедрой Калитина В.В., канд. пед. наук, доцент«10» 02 2026 г.

* - В качестве рецензентов могут выступать работодатели, вузы по профилю, НИИ

Лист согласования рабочей программы

Программа принята методической комиссией института экономики и управления АПК

протокол № 6 « 24 » 02 2026 г.

Председатель методической комиссии Института экономики и управления канд.эконом.наук, доцент Далисова Н.А. « 24» 02 2026 г.

Заведующий выпускающей кафедрой по специальности 09.02.11 Разработка и управление программным обеспечением

Калитина В.В., канд. пед. наук, доцент
(ФИО, ученая степень, ученое звание)

« 24» 04 2026 г.

Содержание

Аннотация 5
1. Цель и место дисциплины в структуре образовательной программы 5
2. Задачи дисциплины. Планируемые результаты освоения дисциплины 6
3. Организационно-методические данные дисциплины 8
4. Содержание дисциплины 8
4.1 Трудоёмкость модулей и модульных единиц дисциплины 8
4.3. Лекционные/лабораторные/практические/семинарские занятия 10
4.4. Лабораторные/практические/семинарские занятия 12
4.5. Самостоятельное изучение разделов дисциплины и виды самоподготовки к текущему контролю знаний 13
5. Взаимосвязь видов учебных занятий 13
6. Учебно-методическое и информационное обеспечение дисциплины 14
6.1. Карта обеспеченности литературой 14
6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет» 15
6.3 Программное обеспечение 15
7. Критерии оценки знаний, умений, навыков и заявленных компетенций 16
7.1 Календарный модуль (3 семестр) 16
8. Материально-техническое обеспечение дисциплины 17
9. Методические рекомендации для обучающихся по освоению дисциплины 18
9.1. Методические указания по дисциплине для обучающихся 18
9.2. Методические указания по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья 19

Общая характеристика РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОП.05 Основы информационной безопасности»

Аннотация

Дисциплина «Основы информационной безопасности» является дисциплиной общепрофессионального цикла учебного плана подготовки студентов по специальности 09.02.11 Разработка и управление программным обеспечением. Дисциплина реализуется в институте Экономики и управления АПК кафедрой Информационных технологий и математического обеспечения информационных систем.

Дисциплина нацелена на формирование профессиональных компетенций выпускника:

ОК 01 - Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам

ПК 1.5 - Защищать информацию в базе данных с использованием технологии защиты информации

ПК 3.3 - Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием

Содержание дисциплины:

- Основные понятия и задачи информационной безопасности
- Основы защиты информации
- Угрозы безопасности защищаемой информации
- Методология защиты информации

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, выполнения заданий лабораторных работ и промежуточная аттестация в форме зачета, зачета с оценкой.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы, 32 часа. Программой дисциплины предусмотрены лекции (16 часов), практические работы (16 часов) занятия.

Используемые сокращения

ФГОС СПО – Федеральный государственный образовательный стандарт среднеспециального образования
ОПОП – основная профессиональная образовательная программа
Л – лекции
ЛЗ – лабораторные занятия
ПЗ – практические занятия
С – семинары
СРС – самостоятельная работа студентов

1. Цель и место дисциплины в структуре образовательной программы

Цель дисциплины «ОП.05 Основы информационной безопасности»: формирование представлений области информационной безопасности, определяющей потребности в развитии интереса к изучению учебных дисциплин и профессиональных модулей, способности к личному самоопределению и самореализации в учебной деятельности.

Дисциплина «Основы информационной безопасности» может быть использована в ряде вопросов прохождения преддипломной практики и при выполнении и защите выпускной квалификационной работы.

2. Задачи дисциплины. Планируемые результаты освоения дисциплины

Задачи изучения дисциплины: после изучения дисциплины студент должен обладать специальной подготовкой в предметной области, знать принципы организации информационной безопасности и методы защиты информации, знать международные стандарты информационного обмена.

Результаты освоения дисциплины соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника.
В результате освоения дисциплины обучающийся должен:

Таблица 1

Перечень планируемых результатов обучения по дисциплине

Код компетенции	Содержание компетенции	Перечень планируемых результатов обучения по дисциплине
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	***Знает*** контекст деятельности, алгоритмы решения задач, источники информации, методы работы, порядок оценки результатов ***Умеет*** распознавать задачи, составлять планы, искать информацию, применять методы, оценивать результаты ***Владеет*** выбором способов решения задач ИБ, планированием, оценкой эффективности
ПК 1.5	Защищать информацию в базе данных с использованием технологии защиты информации	***Знает*** методы защиты БД, криптография, аутентификация, контроль доступа, защита от атак, резервное копирование, облачная безопасность ***Умеет*** настраивать защиту БД, управлять доступом, шифровать данные, проводить аудит, создавать бэкапы, защищать от SQL-инъекций ***Владеет*** навыками по защите БД от НСД, резервным копированием, аудитом безопасности БД
ПК 3.3	Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием	***Знает*** принципы безопасности ИС, методы и технологии защиты, нормативные акты, анализ требований, проектирование, тестирование ***Умеет*** анализировать требования, разрабатывать подсистемы безопасности, тестировать и отлаживать, применять современные методы ***Владеет*** навыками по разработке подсистем безопасности ИС, применением современных методов, оптимизацией

3. Организационно-методические данные дисциплины

Общая трудоемкость дисциплины составляет 3 зач. ед. (32 часа), их распределение по видам работ и по семестрам представлено в таблице 2

Таблица 2

Распределение трудоемкости дисциплины по видам работ по семестрам

Вид учебной работы	Трудоемкость		
	зач. ед.	час	по семестрам
			№ 3
Общая трудоемкость дисциплины по учебному плану	**3**	**32**	**32**
Контактная работа	**3**	**32**	**32**
в том числе:			
Лекции (Л) / в том числе в интерактивной форме	1,5	16	16
Практические занятия (ПЗ) / в том числе в интерактивной форме	1,5	16	16
Семинары (С) / в том числе в интерактивной форме			
Лабораторные работы (ЛР) / в том числе в интерактивной форме			
Самостоятельная работа (СРС)	-	-	-
в том числе:			
самостоятельное изучение тем и разделов			
контрольные работы			
реферат			
самоподготовка к текущему контролю знаний			
др виды			
подготовка к зачету с оценкой	0,3	9	0
Вид контроля:			Зачет с оценкой

4. Содержание дисциплины

4.1 Трудоёмкость модулей и модульных единиц дисциплины

Таблица 3

Трудоемкость модулей и модульных единиц дисциплины

Наименование модулей и модульных единиц дисциплины	**Всего часов на модуль**	**Контактная работа**		**Внеаудиторная работа (СРС)**
		Л	**ЛПЗ**	
Календарный модуль 1. Теоретические основы информационной безопасности	**16**	**8**	**8**	**-**
Модульная единица 1.1 Основные понятия и задачи информационной безопасности	2	2	-	-
Модульная единица 1.2 Основы защиты информации	6	2	4	-
Модульная единица 1.3 Угрозы безопасности защищаемой информации.	8	4	4	-
Календарный модуль 2. Методология защиты информации	**16**	**8**	**8**	**-**

Наименование модулей и модульных единиц дисциплины	Всего часов на модуль	Контактная работа		Внеаудиторная работа (СРС)
		Л	ЛПЗ	
Модульная единица 2.1 Методологические подходы к защите информации	4	2	2	-
Модульная единица 2.2 Нормативно правовое регулирование защиты информации	6	3	3	-
Модульная единица 2.3 Защита информации в автоматизированных (информационных) системах	6	3	3	-
ИТОГО	**32**	**16**	**16**	**-**

4.2 Содержание модулей дисциплины

Раздел 1. Теоретические основы информационной безопасности

Тема 1.1. Основные понятия и задачи информационной безопасности

Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем.

Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности.

Тема 1.2. Основы защиты информации

Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации.

Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.

Цели и задачи защиты информации. Основные понятия в области защиты информации.

Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие политики безопасности.

Тема 1.3. Угрозы безопасности защищаемой информации

Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к уязвимости информации. Методы оценки уязвимости информации

Определение угроз объекта информатизации и их классификация

Раздел 2. Методология защиты информации

Тема 2.1. Методологические подходы к защите информации

Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации.

Тема 2.2. Нормативно правовое регулирование защиты информации

Организационная структура системы защиты информации Законодательные акты в области защиты информации.

Российские и международные стандарты, определяющие требования к защите информации.

Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации

Тема 2.3. Защита информации в автоматизированных (информационных) системах

Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.

Программные и программно-аппаратные средства защиты информации Инженерная защита и техническая охрана объектов информатизации

Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.

4.3. Лекционные/лабораторные/практические/семинарские занятия

Таблица 4

Содержание лекционного курса

№ п/п	№ модуля и модульной единицы дисциплины	№ и тема лекции	Вид[1] контрольного мероприятия	Кол-во часов
1	**Календарный модуль 1. Теоретические основы информационной безопасности**			
1	**Модульная единица 1.1.** Основные понятия и задачи информационной безопасности	Лекция №1,2 Понятие информационной безопасности. Задачи информационной безопасности. Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий.	опрос, тестирование	2
2	**Модульная единица 1.2**. Основы защиты информации	Лекция №3,4 Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи защиты информации. Основные понятия в области защиты информации. Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие политики безопасности.	опрос, тестирование	2
3	**Модульная единица 1.3**. Угрозы безопасности защищаемой информации.	Лекция №5,6,7,8 Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к уязвимости информации. Методы оценки уязвимости информации	опрос, тестирование	4

[1]**Вид мероприятия:** тестирование, коллоквиум, зачет, экзамен, другое4

№ п/п	№ модуля и модульной единицы дисциплины	№ и тема лекции	Вид[1] контрольного мероприятия	Кол-во часов
		Определение угроз объекта информатизации и их классификация		
	Календарный модуль 2. Методология защиты информации			
6	**Модульная единица 2.1. Методологические подходы к защите информации**	Лекция №9,10 Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации.	опрос, тестирование	2
7	**Модульная единица 2.2**. Нормативно правовое регулирование защиты информации	Лекция №11-13 Организационная структура системы защиты информации Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации	опрос, тестирование	3
8	**Модульная единица 2.3.** Защита информации в автоматизированных (информационных) системах	Лекция №14-16 Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах. Программные и программно-аппаратные средства защиты информации Инженерная защита и техническая охрана объектов информатизации Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.	опрос, тестирование	3
	Итого		Зачет с	16

№ п/п	№ модуля и модульной единицы дисциплины	№ и тема лекции	Вид[1] контрольного мероприятия	Кол-во часов
			оценкой	
Интерактивные формы обучения: диалоговое обсуждение отдельных вопросов, совместное (групповое) решение типовых задач				

4.4. Лабораторные/практические/семинарские занятия

Таблица 5

Содержание занятий и контрольных мероприятий

№ п/п	№ модуля и модульной единицы дисциплины	№ и название лабораторных/ практических занятий с указанием контрольных мероприятий	Вид[2] контрольного мероприятия	Кол-во часов
	Календарный модуль 1. Теоретические основы информационной безопасности			
1	**Модульная единица 1.2**. Основы защиты информации	Работа №1-4 Анализ жизненного цикла конфиденциальной информации и классификация угроз на каждом этапе. Разработка фрагмента политики информационной безопасности организации для защиты конфиденциальной информации. Моделирование нарушения целостности, доступности и конфиденциальности и анализ последствий	Практическая работа	4
2	**Модульная единица 1.3**. Угрозы безопасности защищаемой информации.	Работа №5-8 Выявление и классификация каналов несанкционированного доступа на объекте информатизации. Классификация угроз безопасности информации для типового объекта информатизации. Оценка уязвимостей информации и выбор методов их устранения. Анализ угроз объекта информатизации и разработка	Практическая работа	4

[2]**Вид мероприятия:** тестирование, коллоквиум, зачет, экзамен, другое

№ п/п	№ модуля и модульной единицы дисциплины	№ и название лабораторных/ практических занятий с указанием контрольных мероприятий	Вид[2] контрольного мероприятия	Кол-во часов
		мер защиты на основе системной классификации		
	Календарный модуль 2. Методология защиты информации			
6	**Модульная единица 2.1.** Методологические подходы к защите информации	Работа №9-10 Анализ методик определения требований к защите информации для типовой организации. Оценка факторов, влияющих на требуемый уровень защиты информации, и выбор мер защиты	Практическая работа	2
7	**Модульная единица 2.2**. Нормативно правовое регулирование защиты информации	Работа №11-13 Анализ организационной структуры системы защиты информации типовой организации. Сравнительный анализ российских законодательных актов и стандартов в области защиты информации. Изучение системы сертификации РФ в области защиты информации.	Практическая работа	3
8	**Модульная единица 2.3.** Защита информации в автоматизированных (информационных) системах	Работа № 14-16 Комплексный анализ и подбор мер защиты информации для автоматизированной системы типовой организации. Разработка фрагмента организационно-распорядительной системы защиты информации	Практическая работа	3
	Итого		Зачет с оценкой	**16**
Интерактивные формы обучения: диалоговое обсуждение отдельных вопросов, совместное (групповое) решение типовых задач				

4.5. Самостоятельное изучение разделов дисциплины и виды самоподготовки к текущему контролю знаний

Самостоятельная работа учебным планом не предусмотрена.

5. Взаимосвязь видов учебных занятий

Взаимосвязь учебного материала лекций, лабораторных работ с тестовыми вопросами и формируемыми компетенциями представлены в таблице 6.

Таблица 6

Взаимосвязь компетенций с учебным материалом и контролем знаний студентов

Компетенции	Лекции	ЛЗ	СРС	Другие виды	Вид контроля
ОК 01	1-16	1-16	-		Зачет с оценкой
ПК-1.5	1-16	1-16	-		Зачет с оценкой
ПК-3.3	1-16	1-16	-		Зачет с оценкой

6. Учебно-методическое и информационное обеспечение дисциплины
6.1. Карта обеспеченности литературой

Кафедра Информационные технологии и математическое обеспечение информационных систем
09.02.11 «Разработка и управление программным обеспечением»
Дисциплина Основы информационной безопасности

Вид занятий	Наименование	Авторы	Издательство	Год издания	Вид издания		Место хранения		Необходи-мое количество экз.	Количество экз. в вузе
					Печ.	Электр.	Библ.	Каф.		
1	2	3	4	6	7	8	9	10	11	12
Основная										
Лекции, лаборат. работы.	Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования	Внуков, А. А	Москва: Издательство Юрайт	2024		Электр	Библ			https://urait.ru/bcode/542340
Лекции, лаборат. работы..	Основы информационной безопасности: надежность и безопасность программного обеспечения: учебник для среднего профессионального образования	Казарин, О. В.	Москва: Издательство Юрайт	2025		Электр	Библ			https://znanium.com/catalog/product/1910870
Дополнительная										
Лекции, лаборат. работы.	Основы информационной безопасности : учебник для СПО	Нестеров, С. А.	Санкт-Петербург : Лань	2022		Электр.	Библ.		8	https://e.lanbook.com/book/195510

Директор Научной библиотеки

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Интернет-ресурсы

1. Хранилища данных. Электронный обучающий ресурс https://e.kgau.ru/enrol/index.php?id=1059 (Moodle)
2. Национальный Открытый Университет «ИНТУИТ» https://intuit.ru/
3. Портал CIT Forum http://citforum.ru/
4. Информационно-аналитическая система «Статистика» http://www.ias-stat.ru/

Электронные библиотечные системы

1. Каталог библиотеки Красноярского ГАУ - https://kgau.ru/library/elektronnye-resursy/
2. ЭБС Издательства «Лань», адрес сайта: http://e.lanbook.com (договор № 45 от 10.03.2021); (договор №13/4-21 от 03.09.2021); (договор №21/5-22 от 05.03.2022); (договор №1 от 19.03.2023); (договор №2 от 19.03.2023); (Договор №1/14-24 от 29.02.2024); (№2/14-24 от 04.03.2024); (№1/14-25 от 17.02.2025); (№2/14-25 от 17.02.2025); (договор №1/14-26 от 26.02.2026); (договор №2/14-26 от 26.02.2026)
3. ЭБС издательства «Юрайт», адрес сайта https://urait.ru/ (договор №10/4-21 от 31.03. 2021); (договор №12/4-21 от 16.06. 2021); (договор №5293 от 23.05.2022); (договор №5857 от 16.05.2023); (договор №36/4-24 от 15.05.2024, договор №3-14-25 от 25.06.25).
4. ЭБС Руконт, адрес сайта https://lib.rucont.ru/ (Издательство Колосс «Сельское хозяйство», научные монографии) (договор №18/4-23 от 01.03.2023); (№32/4-23 от 02.10.2023); (№16/4-24 от 20.02.2024); (№6/4-25 от 24.02.2025)
5. Коллекция электронных изданий Сибирского федерального университета (договор о сотрудничестве № 200/10-20 от 25.09.2020 ФГАОУ ВО «Сибирский федеральный университет»)
6. Национальная электронная библиотека https://rusneb.ru/ (договор №101/НЭБ/2276 о предоставлении доступа к от 06.06.2017 ФГБУ «РГБ»)
7. Электронная библиотека Красноярского ГАУ ИРБИС64+ http://5.159.97.194:8080/cgi-bin/irbis64r_plus/irbis_webcgi.exe?C21COM=F&I21DBN=IBIS_FULLTEXT&P21DBN=IBIS&Z21ID=&S21CNR=5
8. Электронный каталог Государственной универсальной научной библиотеки Красноярского края - https://irbis.kraslib.ru/?C21COM=F&I21DBN=EKU&P21DBN=EKU&S21CNR=20&Z21ID= /
9. Научная электронная библиотека «КиберЛенинка». https://cyberleninka.ru
10. Lens.org https://www.lens.org
11. Bielefeld Academic Search Engine https://www.base-search.net
12. OpenAlexhttps://openalex.org
13. Wiley https://onlinelibrary.wiley.com/
14. Национальный агрегатор открытых репозиториев https://www.openrepository.ru/

Информационно-справочные системы

1. Информационно-правовой портал «Гарант». http://www.garant.ru/(договор №248/10-21 об информационно-правовом сотрудничестве от 29.03.2021)
2. Справочно-правовая система «Консультант +» https://www.consultant.ru (договор №20059900202 об информационной поддержке от 02.03.2015 ООО Информационный центр «Искра»;

Профессиональные базы данных

1. Коллективный блог по информационным технологиям, бизнесу и интернету. https://habr.com/ru/
2. OpenNet. Адрес ресурса: http://www.opennet.ru/

6.3 Программное обеспечение

Лицензионное ПО Красноярского ГАУ

1. Операционная система AstraLinux (лицензия № 192400033-alse-1.7-client-base_orel-x86_64-0-12913 от 28.08.2023).
2. Офисный пакет приложений LibreOffice входит в комплект поставки AstraLinux.
3. Офисный пакет приложений Мой Офис (лицензия № ПР0000-35377 от 24.07.2024).
4. 1С Предприятие 8.2 (акт предоставления прав № Тг059122 от 24.10.2012).
5. Справочная правовая система "Консультант+" (договор №20059900202 об информационной поддержке от 02.03.2015 ООО Информационный центр «Искра»).
6. Moodle 3.5.6a (договор № 969.2 от 17.04.2020).

Свободно-распространяемое ПОили бесплатная лицензия с открытым исходным кодом:

1. ГИС Панорама x64 версия 15 мультиплатформенная лицензия (104622 фиксированная лицензия)
2. PostgreSQL; SWI-Prolog, Ramus Educational; StarUML; XMind v3.0; QT Creater, Oracle VM Virtual Box;DBeaver Community; MySQL Community Edition; Gimp; Wireshark; Graphical Network Simulator-3; NASM; SMath Studio; OpenJDK; Notepad++; LibreCad; Yandex (браузер).

7. Критерии оценки знаний, умений, навыков и заявленных компетенций

7.1 Календарный модуль (3 семестр)

Текущая аттестация обучающихся производится в дискретные временные интервалы преподавателем, ведущим занятия по дисциплине, в следующих формах:

- тестирование;
- опрос
- выполнение практических работ
- отдельно оцениваются личностные качества студента (аккуратность, исполнительность, инициативность) – работа у доски, своевременная сдача тестов.

Рейтинг – план дисциплины «Основы информационной безопасности»

	Модули	Часы	Баллы
1	Календарный модуль	99	80
	Зачёт с оценкой	9	20
	Итого	**108**	**100**

Распределение баллов по модулям

№	Модули	Баллы по видам работ				Итого
		Опрос	Тестирование	Выполнение лабораторных работ	Итоговое тестирование (Зачёт)	
1	Календарный модуль № 1	10	30	40		80
	Зачёт	-	-	-	20	20
	Итого	**10**	**30**	**40**	**20**	**100**

Оценочные средства по всем видам текущей работы и промежуточной аттестации, а также критерии оценивания приведены в ФОС по дисциплине «Основы информационной безопасности».

Промежуточный контроль *зачет с оценкой* по результатам 3 семестра по дисциплине проходит в форме контрольного итогового тестирования.

Если студент набрал 60 баллов в течение срока изучения дисциплин, то зачет выставляется автоматически.

Если студент набрал менее 60 баллов в течении срока изучения дисциплин, то студент проходит контрольное итоговое тестирование, которое осуществляется по следующим критериям:

Обучающийся, давший правильные ответы 87-100% тестирующих материалов (1-5 ошибок), получает максимальное количество баллов – 20.

Обучающийся, давший правильные ответы в пределах 73-86% тестирующих материалов (6-10 ошибок), получает 15 баллов.

Обучающийся, давший правильные ответы в пределах 60-72% (11-15 ошибок) тестирующих материалов, получает 10 баллов.

Баллы, полученные на итоговом тестировании, суммируются с баллами, полученными в течение семестра на текущей аттестации, и выводится итоговая оценка по зачёту по следующим критериям:

Оценка «отлично» выставляется студенту, если сумма баллов, набранных в ходе текущего контроля и промежуточного контроля, составляет от 87 до 100 баллов.

Оценка «хорошо» выставляется студенту, если сумма баллов, набранных в ходе текущего контроля и промежуточного контроля, составляет менее 75-86 баллов

Оценка «удовлетворительно» выставляется студенту, если сумма баллов, набранных в ходе текущего контроля и промежуточного контроля, составляет менее 60-74 балла

Оценка «не зачтено» ставится, если студент не набрал 60 баллов.

Обучающийся, не сдавший зачёт, приходит на пересдачу в сроки в соответствии с графиком ликвидации академических задолженностей: http://www.kgau.ru/new/news/news/2017/grafik_lz.pdf.

8. Материально-техническое обеспечение дисциплины

Виды занятий	Аудиторный фонд
Лекции	Занятия лекционного типа проводятся в аудиториях оснащенных комплектом мультимедийного оборудования (стационарного/переносного) с выходом в локальную сеть и Интернет. Рабочие места преподавателя и бакалавров (магистрантов), укомплектованные специализированной мебелью, и техническими средствами обучения, служащими для представления учебной информации большой аудитории., Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, аудиторная доска, общая локальная компьютерная сеть Internet, компьютер Intel i5 12400/16Гб/DDR4, монитор LG 24MP400-B. Телевизор LED 65" TCL 65C735
Лабораторные/практические работы	Лабораторные работы проводятся в компьютерном классе, имеющий достаточное количество посадочных мест для размещения студентов и оснащенным наборами демонстрационного оборудования и учебно-наглядных пособий; рабочие места преподавателя и студентов укомплектованы специализированной мебелью и техническими средствами обучения; общая локальная компьютерная сеть Internet; 15 компьютеров Intel i5 12400/16Гб/DDR4, монитор TeslaF2422HF.
Самостоятельная работа	Помещение для самостоятельной работы 3-13 (660130, Красноярский край, г. Красноярск, ул. Елены Стасовой 44 «И») - рабочие места укомплектованны специализированной мебелью; общая локальная компьютерная сеть Internet; 11 компьютеров Core2 Duo E7400/ESC/2Gb/DVD+RW, монитор Samsung 2233SN. Телевизор BlacktonBt 50FSU32B.

	Помещение для самостоятельной работы 1-06 (660130, Красноярский край, г. Красноярск, ул. Елены Стасовой, 44 «Г») - Информационно-ресурсный центр Научной библиотеки - 14 посадочных мест: рабочие места студентов, укомплектованные специализированной мебелью, Гигабитный интернет, 10компьютеров на базе процессора IntelCore i3 в комплектации с монитором Samsung и др. внешними периферийными устройствами ((инв.№ 1101040757, 1101040761, 1101040767, 1101040768, 1101040775, 2101040032, 2101040034, 2342009415, 2342009416, 2342011415), мультимедийный комплектPanasonic(проектор, экран) №11024274, МФУ LaserJet M1212 № 2342077033. Помещение для самостоятельной работы 2-03 (660130, Красноярский край, г. Красноярск, ул. Елены Стасовой, 44 «Г») - на 51 посадочное место: рабочие места магистрантов, укомплектованные специализированной мебелью, Гигабитный интернет, Wi-fi, 6 компьютеров на базе процессора IntelCore i3 в комплектации с монитором Samsung и др. внешними периферийными устройствами (инв.№ 11014350,11014533, 11014604, 1101040765, 2101040031, 4342025164), мультимедийный проектор Acer X 1260P №2101040044, экран №2101040047, телевизор Samsung№4342017001, телевизор SBER SDX-75UQ5233 №43420251038

9. Методические рекомендации для обучающихся по освоению дисциплины

9.1. Методические указания по дисциплине для обучающихся

Курс “Основы информационной безопасности” базируется и требует предварительного знания таких дисциплин как «Информатика», «Математика», «Алгоритмизация и программирование».

Дисциплина «Основы информационной безопасности» является основополагающим для изучения следующих дисциплин: «Управление IT-проектами», «Разработкам интеграция модумей программного обеспечения». В процессе изучения дисциплины студенты развивают, расширяют и углубляют знания в области компьютерной защиты информации.

Успешное изучение курса требует от студентов посещения лекций, активной работы на практических занятиях, выполнения всех учебных заданий преподавателя, ознакомления с базовыми учебниками, основной и дополнительной литературой. Запись лекции – одна из форм активной самостоятельной работы студентов, требующая навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки. Для конспектирования лекций рекомендуется создать собственную удобную систему сокращений, аббревиатур и символов.

Лекции нацелены на освещение наиболее трудных вопросов, а также призваны способствовать формированию навыков работы с литературой.

При изучении дисциплины для улучшения качества учебного процесса преподаватели используют демонстрацию основных принципов работы на компьютере с использованием мультимедийных средств и презентаций, сопровождая информационный материал комментариями, что позволяет внести позитивное разнообразие в учебный процесс и способствует повышению знаний студентов.

Основной формой проведения практических занятий является выполнение конкретных заданий в виде лабораторных работ на компьютерах.

Лабораторно-практическое занятие - это форма организации учебного процесса, предполагающая выполнение студентами по заданию и под руководством преподавателя одной или нескольких работ. И если на лекции основное внимание студентов сосредотачивается на разъяснении теории конкретной учебной дисциплины, то практические занятия служат для обучения методам ее применения. Главной целью практических занятий является усвоение метода использования теории, приобретение профессиональных умений, а также практических умений, необходимых для изучения последующих дисциплин.

Кроме того, для закрепления навыков работы с компьютерами, студенты занимаются самостоятельно с имеющимися программами и изучают теоретические вопросы.

Полученные навыки и знания помогут студентам в условиях развития информационных технологий быстро и профессионально ориентироваться в новых подходах, которые возникают в связи с увеличением возможностей вычислительной техники. Возрастающие возможности вычислительной техники порождают новые концепции и подходы в системе учёта, хранения, обработки, преобразования информации, её безопасности. В свою очередь новые концепции и подходы стимулируют создание новых информационных систем, которые должны быстро внедряться в практическую и хозяйственную деятельность государственных и частных структур. Поэтому курс построен так, что помимо конкретных базовых знаний, студенту предлагаются некоторые схемы и методики, которые помогут развить самостоятельные навыки в изучении нового материала. Это позволяет студенту повысить профессиональный кругозор, а преподавателю моделировать реальные ситуации, которые могут возникнуть при переходе студента от учёбы к практической деятельности.

Обязательными видами промежуточной аттестации, без наличия которых студенты не допускаются до зачета и зачета с оценкой, является выполнение всех лабораторно-практических заданий.

Студент может быть освобожден преподавателем от промежуточной и окончательной аттестации при активной работе во время практических занятий, при участии в студенческих научных конференциях по тематике предмета.

9.2. Методические указания по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья

В целях освоения учебной программы дисциплины инвалидами и лицами с ограниченными возможностями здоровья обеспечивается:

1. Для инвалидов и лиц с ограниченными возможностями здоровья по зрению:

1.1. размещение в доступных для обучающихся местах и в адаптированной форме справочной информации о расписании учебных занятий;

1.2. присутствие ассистента, оказывающего обучающемуся необходимую помощь;

1.3. выпуск альтернативных форматов методических материалов (крупный шрифт или аудиофайлы);

2. Для инвалидов и лиц с ограниченными возможностями здоровья послуху:

2.1. надлежащими звуковыми средствами воспроизведение информации;

3. Для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата:

3.1. возможность беспрепятственного доступа обучающихся в учебные помещения, туалетные комнаты и другие помещения института, а также пребывание в указанных помещениях.

Образование обучающихся с ограниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и в отдельных группах или в отдельных организациях.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются водной из форм, адаптированных к ограничениям их здоровья и восприятия информации.

Категории студентов	Формы
С нарушение слуха	• в печатной форме; • в форме электронного документа;
С нарушением зрения	в печатной форме увеличенных шрифтом; в форме электронного документа; в форме аудиофайла;

С нарушением опорно-двигательного аппарата	в печатной форме; в форме электронного документа; в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы, и индивидуальная воспитательная работа. Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

ПРОТОКОЛ ИЗМЕНЕНИЙ РПД

Дата	Раздел	**Изменения**	Комментарии
		1.1.1	

Программу разработали:

Романова Дарья Сергеевна, ст. преподаватель