

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего
образования «Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Директор Таганрогского института
имени А.П. Чехова (филиала)
РГЭУ (РИНХ)
_____ Голобородько А.Ю.
« ____ » _____ 20__ г.

**Рабочая программа дисциплины
Информационная безопасность**

направление 44.03.05 Педагогическое образование (с двумя профилями подготовки)
направленность (профиль) 44.03.05.35 Биология и Безопасность жизнедеятельности

Для набора _____ года

Квалификация
Бакалавр

КАФЕДРА информатики**Распределение часов дисциплины по семестрам**

Семестр (<Курс>. <Семестр на курсе>)	7 (4.1)		Итого	
	17			
Неделя	17			
Вид занятий	уп	рп	уп	рп
Лекции	16	16	16	16
Лабораторные	16	16	16	16
Итого ауд.	32	32	32	32
Контактная работа	32	32	32	32
Сам. работа	40	40	40	40
Итого	72	72	72	72

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 30.08.2021 протокол № 1.

Программу составил(и): канд. техн. наук, Доц., Усенко Ольга Александровна _____

Зав. кафедрой: Тюшнякова И.А. _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Целью освоения дисциплины «Информационная безопасность» является формирование у обучаемых знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.
-----	---

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

УК-4.1: Использует различные формы, виды устной и письменной коммуникации на русском, родном и иностранном(ых) языке(ах)
УК-4.2: Свободно воспринимает, анализирует и критически оценивает устную и письменную деловую информацию на русском, родном и иностранном(ых) языке(ах)
УК-4.3: Владеет системой норм русского литературного языка, родного языка и нормами иностранного(ых) языка (ов)
УК-4.4: Использует языковые средства для достижения профессиональных целей на русском, родном и иностранном(ых) языке(ах)
УК-4.5: Выстраивает стратегию устного и письменного общения на русском, родном и иностранном(ых) языке(ах)в рамках межличностного и межкультурного общения
УК-1.1: Демонстрирует знание особенностей системного и критического мышления и готовности к нему
УК-1.2: Применяет логические формы и процедуры, способен к рефлексии по поводу собственной и чужой мыслительной деятельности
УК-1.3: Анализирует источник информации с точки зрения временных и пространственных условий его возникновения
УК-1.4: Анализирует ранее сложившиеся в науке оценки информации
УК-1.5: Сопоставляет разные источники информации с целью выявления их противоречий и поиска достоверных суждений
УК-1.6: Аргументированно формирует собственное суждение и оценку информации, принимает обоснованное решение
УК-1.7: Определяет практические последствия предложенного решения задачи
ОПК-9.1: Использует современные информационные технологии при решении задач профессиональной деятельности и понимает принципы их работы
ОПК-9.2: Обоснованно выбирает современные информационные технологии, ориентируясь на задачи профессиональной деятельности
ОПК-9.3: Владеет навыками применения современных информационных технологий для решения задач профессиональной деятельности

В результате освоения дисциплины обучающийся должен:

Знать:
правовые понятия и нормы Российского законодательства, иметь представление о системе норм Российского законодательства, о структуре Российского законодательства, видах правовых отраслей и особенностях их регулирования, понимать сущность, характер и взаимодействие правовых явлений, видеть их взаимосвязь в целостной системе знаний и значений реализации права; - правовое обеспечение информационной безопасности переработки информации в ИС; организационно-правовые основы защиты информационных ресурсов предприятия; теоретические и практические знания по правовым основам защиты информации при работе на вычислительной технике и в каналах связи; нормативно-правовые документы в области информационных систем и технологий; методы и алгоритмы решения стандартных задач в своей профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, знает основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.
Уметь:
анализировать и оценивать нормативно-правовую информацию; планировать и осуществлять свою деятельность с учётом результатов этого анализа; использовать и составлять нормативно-правовые документы, относящиеся к будущей профессиональной деятельности; - находить нужную статью в законе; -самостоятельно анализировать правовую и научную литературу и делать обоснованные выводы; организовывать защиту информации в ИС; применять действующую законодательную базу в области информационной безопасности; разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации; применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы; решать стандартные профессиональные задачи с применением естественнонаучных и инженерных знаний, методов математического анализа и моделирования.

Владеть:

способностью использовать основы правовых знаний в различных сферах деятельности; навыками по предоставлению и улучшению проведения мер по обеспечению безопасности; - правовыми средствами обеспечения информационной безопасности;

навыками работы с нормативно-правовыми документами и стандартами в области информационных систем и технологий, обеспечения требований информационной безопасности;

навыками применения моделей и методов расчета надежности и безопасности информационных систем при различных видах угроз и моделей поведения нарушителя.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература
	Раздел 1. Информационная безопасность				
1.1	Введение в дисциплину. Основные понятия и определения информационной безопасности. Информация и информационная безопасность. Основные составляющие информационной безопасности. Объекты защиты. Категории и носители информации. Средства защиты информации. Способы передачи конфиденциальной информации на расстоянии. /Лек/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-1.4 УК-1.5 УК-1.6 УК-1.7 УК-4.1 УК-4.2 УК-4.3 УК-4.4 УК-4.5 ОПК-9.1 ОПК-9.2 ОПК-9.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.2	Изучение содержания и последовательности работ по защите информации. /Лаб/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-1.4 УК-1.5 УК-1.6 УК-1.7 УК-4.1 УК-4.2 УК-4.3 УК-4.4 УК-4.5 ОПК-9.1 ОПК-9.2 ОПК-9.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.3	Виды угроз информационной безопасности. Модель нарушителя информационной безопасности. /Лек/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-1.4 УК-1.5 УК-1.6 УК-1.7 УК-4.1 УК-4.2 УК-4.3 УК-4.4 УК-4.5 ОПК-9.1 ОПК-9.2 ОПК-9.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.4	Изучение методов комплексного исследования объекта информатизации. /Лаб/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-1.4 УК-1.5 УК-1.6 УК-1.7 УК-4.1 УК-4.2 УК-4.3 УК-4.4 УК-4.5 ОПК-9.1 ОПК-9.2 ОПК-9.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2

1.5	Принципы построения системы защиты информации. Методы защиты. /Лек/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-1.4 УК-1.5 УК-1.6 УК-1.7 УК-4.1 УК-4.2 УК-4.3 УК-4.4 УК-4.5 ОПК-9.1 ОПК-9.2 ОПК-9.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.6	Изучение методов построения систем обеспечения информационной безопасности на основе нормативных актов. Изучение правовой стороны информационной безопасности, идея сертификации и электронной подписи. /Лаб/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-1.4 УК-1.5 УК-1.6 УК-1.7 УК-4.1 УК-4.2 УК-4.3 УК-4.4 УК-4.5 ОПК-9.1 ОПК-9.2 ОПК-9.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.7	Методы и средства защиты информации от шпионажа и несанкционированного доступа. /Лек/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-1.4 УК-1.5 УК-1.6 УК-1.7 УК-4.1 УК-4.2 УК-4.3 УК-4.4 УК-4.5 ОПК-9.1 ОПК-9.2 ОПК-9.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.8	Разработка политики информационной безопасности для организации. /Лаб/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-1.4 УК-1.5 УК-1.6 УК-1.7 УК-4.1 УК-4.2 УК-4.3 УК-4.4 УК-4.5 ОПК-9.1 ОПК-9.2 ОПК-9.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.9	Изучение и построение модели нарушителя информационной безопасности. /Лаб/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-1.4 УК-1.5 УК-1.6 УК-1.7 УК-4.1 УК-4.2 УК-4.3 УК-4.4 УК-4.5 ОПК-9.1 ОПК-9.2 ОПК-9.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.10	Обеспечение информационной безопасности за счет повышения связности телекоммуникационной сети. /Лаб/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-1.4 УК-1.5 УК-1.6 УК-1.7 УК-4.1 УК-4.2 УК-4.3 УК-4.4 УК-4.5 ОПК-9.1 ОПК-9.2 ОПК-9.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2

1.11	Повышение надежности информационных систем, как средство обеспечения информационной безопасности. /Лек/	7	4	УК-1.1 УК-1.2 УК-1.3 УК-1.4 УК-1.5 УК-1.6 УК-1.7 УК-4.1 УК-4.2 УК-4.3 УК-4.4 УК-4.5 ОПК-9.1 ОПК-9.2 ОПК-9.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.12	Методы управления средствами сетевой безопасности. /Лек/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-1.4 УК-1.5 УК-1.6 УК-1.7 УК-4.1 УК-4.2 УК-4.3 УК-4.4 УК-4.5 ОПК-9.1 ОПК-9.2 ОПК-9.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.13	Изучение основных видов компьютерных вирусов и способы борьбы с ними. /Лаб/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-1.4 УК-1.5 УК-1.6 УК-1.7 УК-4.1 УК-4.2 УК-4.3 УК-4.4 УК-4.5 ОПК-9.1 ОПК-9.2 ОПК-9.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.14	Поиск надежных каналов передачи информации в телекоммуникационных сетях. /Лаб/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-1.4 УК-1.5 УК-1.6 УК-1.7 УК-4.1 УК-4.2 УК-4.3 УК-4.4 УК-4.5 ОПК-9.1 ОПК-9.2 ОПК-9.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.15	Повышение безопасности и стандарты информационной безопасности. /Лек/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-1.4 УК-1.5 УК-1.6 УК-1.7 УК-4.1 УК-4.2 УК-4.3 УК-4.4 УК-4.5 ОПК-9.1 ОПК-9.2 ОПК-9.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2
1.16	Подготовка к тестированию, лабораторным работам. /Ср/	7	40	УК-1.1 УК-1.2 УК-1.3 УК-1.4 УК-1.5 УК-1.6 УК-1.7 УК-4.1 УК-4.2 УК-4.3 УК-4.4 УК-4.5 ОПК-9.1 ОПК-9.2 ОПК-9.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2

1.17	/Зачёт/	7	0	УК-1.5 УК-1.6 УК-1.7 УК-4.1 УК-4.2 УК-4.3 УК-4.4 УК-4.5 ОПК-9.1 ОПК-9.2 ОПК-9.3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7Л2.1 Л2.2
------	---------	---	---	---	---

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л1.1	Семенов, Вячеслав Алексеевич	Информационная безопасность: учеб. пособие	М.: МГИУ, 2006	2
Л1.2	Спицын В. Г.	Информационная безопасность вычислительной техники: учебное пособие	Томск: Эль Контент, 2011	http://biblioclub.ru/index.php?page=book&id=208694 неограниченный доступ для зарегистрированных пользователей
Л1.3	Филиппов Б. И., Шерстнева О. Г.	Информационная безопасность. Основы надежности средств связи: учебник	Москва Берлин: Директ-Медиа, 2019	http://biblioclub.ru/index.php?page=book&id=499170 неограниченный доступ для зарегистрированных пользователей
Л1.4	Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н.	Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: учебно-методическое пособие	Йошкар-Ола: Поволжский государственный технологический университет, 2019	http://biblioclub.ru/index.php?page=book&id=562246 неограниченный доступ для зарегистрированных пользователей
Л1.5	Ищейнов В. Я.	Информационная безопасность и защита информации: теория и практика: учебное пособие	Москва Берлин: Директ-Медиа, 2020	http://biblioclub.ru/index.php?page=book&id=571485 неограниченный доступ для зарегистрированных пользователей
Л1.6	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2019	http://biblioclub.ru/index.php?page=book&id=576726 неограниченный доступ для зарегистрированных пользователей
Л1.7	Фомин, Д. В.	Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства: учебно-методическое пособие	Саратов: Вузовское образование, 2018	http://www.iprbookshop.ru/77317.html неограниченный доступ для зарегистрированных пользователей
Л1.8	Фаронов, А. Е.	Основы информационной безопасности при работе на компьютере: учебное пособие	Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020	http://www.iprbookshop.ru/89453.html неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1	Артемов А. В.	Информационная безопасность: курс лекций: курс лекций	Орел: Межрегиональная академия безопасности и выживания, 2014	http://biblioclub.ru/index.php?page=book&id=428605 неограниченный доступ для зарегистрированных пользователей
Л2.2	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014	http://biblioclub.ru/index.php?page=book&id=438331 неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

garant.ru

Consultant.ru

5.4. Перечень программного обеспечения

Гарант (учебная версия)

Microsoft Office

5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Помещения для проведения всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения. Для проведения лекционных занятий используется демонстрационное оборудование. Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными программными средствами и выходом в Интернет.

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

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.