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

УТВЕРЖДАЮ
Начальник
учебно-методического управления
Платонова Т.К.
«25» июня 2024 г.

Рабочая программа дисциплины
Информационная безопасность

Направление 38.03.05 Бизнес-информатика
Направленность 38.03.05.02 Информационное и программное обеспечение бизнес-процессов в цифровой экономике

Для набора 2024 года

Квалификация
Бакалавр

КАФЕДРА **Информационная безопасность**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**1 (1.1)**		**2 (1.2)**		Итого	
Недель	16		16			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	16	16	16	16	32	32
Практические	16	16	16	16	32	32
Итого ауд.	32	32	32	32	64	64
Контактная работа	32	32	32	32	64	64
Сам. работа	76	76	184	184	260	260
Часы на контроль			36	36	36	36
Итого	108	108	252	252	360	360

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 25.06.2024 г. протокол № 18.

Программу составил(и): к.т.н., доцент, Севастьянов И.Т.

Зав. кафедрой: к.э.н., доцент Радченко Ю.В.

Методический совет направления: д.э.н., профессор Тищенко Е.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Приобретение знаний в области информационной безопасности и защиты информации по организационно-правовой защите коммерческой, служебной, профессиональной тайны, персональных данных; формирование умений и практических навыков по правовому, организационному и техническому обеспечению защиты информации при решении задач профессиональной деятельности.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-2: Способен управлять ИТ-инфраструктурой предприятия с учетом требований обеспечения информационной безопасности

В результате освоения дисциплины обучающийся должен:

Знать:

- принципы работы современных технологий обеспечения информационной безопасности при решении задач профессиональной деятельности (соотнесено с индикатором ПК-2.1).

Уметь:

- решать стандартные задачи профессиональной деятельности с учетом требований информационной безопасности (соотнесено с индикатором ПК-2.2).

Владеть:

- навыками использования способов и средств защиты информации при решении задач профессиональной деятельности (соотнесено с индикатором ПК-2.2).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Система защиты данных в Российской Федерации

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
1.1	Вводная лекция. Важность защиты информации в современном мире. Ключевые принципы обеспечения информационной безопасности / Лек /	1	2	ПК-2	Л1.1, Л1.2, Л1.3, Л1.5, Л2.1, Л2.4, Л2.5
1.2	Виды информации в зависимости от её содержания, доступа, обладателя / Лек /	1	2	ПК-2	Л1.1, Л1.2, Л1.3, Л1.5, Л2.1, Л2.4, Л2.5
1.3	Основные модели защиты информации. / Лек /	1	2	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.4	Изучение основных положений по защите информации: Доктрина информационной безопасности Российской Федерации. / Ср /	1	2	ПК-2	Л1.1, Л1.2, Л1.3, Л1.5, Л2.1, Л2.4, Л2.5
1.5	Основные положения Федерального закона "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ. Основные принципы и требования к системе защиты данных. Роли и ответственность участников системы защиты данных. / Ср /	1	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
1.6	Выполнение заданий с использованием LibreOffice. / Ср /	1	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

Раздел 2. Основы защиты цифровых данных в киберпространстве

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
2.1	Понятие и виды угроз информационной безопасности. Уязвимости. Управление уязвимостями. / Лек /	1	2	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.2	Компьютерные атаки. Виды и классификация компьютерных атак. / Лек /	1	2	ПК-2	Л1.1, Л1.2, Л1.3, Л1.5, Л2.1, Л2.4,

					Л2.5
2.3	Организация парольной защиты. Парольные атаки. / Лек /	1	2	ПК-2	Л1.1, Л1.2, Л1.3, Л1.5, Л2.1, Л2.4, Л2.5
2.4	Проверка надежности парольной защиты с использованием встроенных инструментов Kali Linux. / Пр /	1	8	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.5	Изучение основных инструментов для выявления уязвимостей. / Пр /	1	8	ПК-2	Л1.1, Л1.2, Л1.3, Л1.5, Л2.1, Л2.4, Л2.5
2.6	Основные типы угроз и их классификация. Угрозы безопасности облачных сервисов. / Ср /	1	8	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.7	Классификация уязвимостей. Уязвимости операционных систем, приложений. сетевого оборудования и протоколов. / Ср /	1	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.8	Компьютерные атаки на беспроводные сети и мобильные устройства. Атаки на веб-приложения и базы данных. Атаки на системы управления доступом и паролями. / Ср /	1	6	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
2.9	Выполнение заданий с использованием LibreOffice. / Ср /	1	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

Раздел 3. Компьютерные вирусы. Основные принципы детектирования вредоносного программного обеспечения (ВПО)

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
3.1	Виды и история развития компьютерных вирусов. Современные тенденции применения компьютерных вирусов. / Лек /	1	2	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
3.2	Принцип работы антивирусных программ. Способы детектирования вредоносного программного обеспечения (ВПО) / Лек /	1	2	ПК-2	Л1.1, Л1.2, Л1.3, Л1.5, Л2.1, Л2.4, Л2.5
3.3	Вредоносное программное обеспечение и методы его обнаружения. / Ср /	1	6	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
3.4	Сигнатурный анализ и эвристический анализ для обнаружения ВПО. Обнаружение и удаление руткитов и троянских программ. Обнаружение и блокировка фишинговых атак. / Ср /	1	8	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
3.5	Выполнение заданий с использованием LibreOffice. / Ср /	1	30	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
3.6	/ Зачёт /	1	0	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

Раздел 4. Организация защиты персональных данных

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
4.1	Персональные данные (ПДн). Виды, классификация персональных данных. Порядок обработки ПДн в информационных системах. / Лек /	2	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
4.2	Обработка персональных данных: основы и практика отзыва согласия на обработку прекратить обработку своих	2	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.5, Л2.1, Л2.4,

	персональных данных у оператора ПДн. / Пр /				Л2.5
4.3	Основы законодательства о защите персональных данных: Права субъектов персональных данных.Ответственность за нарушение законодательства о защите персональных данных. / Ср /	2	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
4.4	Обработка персональных данных: Технические меры защиты персональных данных. Особенности защиты персональных данных в различных отраслях экономики. / Ср /	2	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.5, Л2.1, Л2.4, Л2.5
4.5	Выполнение заданий с использованием LibreOffice. / Ср /	2	36	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

Раздел 5. Организация защиты информации в информационных системах

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
5.1	Информационные системы и организация защиты информации в них. / Лек /	2	2	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
5.2	Управление доступом и контроль авторизации в информационных системах. / Пр /	2	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
5.3	Основные принципы и методы защиты информации в информационных системах. / Ср /	2	6	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
5.4	Программные средства защиты информации в информационных системах. / Ср /	2	6	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
5.5	Обучение персонала и повышение осведомленности в вопросах информационной безопасности. / Ср /	2	6	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

Раздел 6. Основы криптографической защиты и организация использования электронных подписей.

№	Наименование темы / Вид занятия	Семестр / Курс	Часов	Компетен-ции	Литература
6.1	Методы и средства криптографической защиты информации. Принципы функционирования основных криптографических алгоритмов. / Лек /	2	2	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
6.2	Электронная подпись (ЭП). Основные понятия и виды ЭП. Порядок выдачи и проверки ЭП. особенности применения ЭП в электронном документообороте. / Лек /	2	2	ПК-2	Л1.1, Л1.2, Л1.3, Л1.5, Л2.1, Л2.4, Л2.5
6.3	Криптографические протоколы и их применение.Хэширование и цифровые подписи. / Ср /	2	6	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
6.4	Юридические аспекты использования электронных подписей. Безопасность хранения и передачи ключей шифрования. / Ср /	2	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
6.5	Выполнение заданий с использованием LibreOffice. / Ср /	2	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
6.6	Аутентификация и идентификация в системах с использованием электронных подписей. Управление ключами и сертификатами в системах с электронными подписями. / Ср /	2	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

Раздел 7. Основы безопасности объектов критической информационной инфраструктуры.					
№	**Наименование темы / Вид занятия**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**
7.1	Объекты и субъекты критической информационной инфраструктуры (КИИ) Предъявляемые требования к обеспечению безопасности КИИ. Проведение категорирования КИИ. / Лек /	2	2	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
7.2	Государственная система обнаружения и предупреждения компьютерных атак ГосСОПКА. Цели и задачи ГоСОПКА. Техническое оснащение и персонал. / Лек /	2	2	ПК-2	Л1.1, Л1.2, Л1.3, Л1.5, Л2.1, Л2.4, Л2.5
7.3	Законодательство и нормативные акты в области безопасности объектов критической информационной инфраструктуры. / Ср /	2	6	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
7.4	Организационные меры безопасности объектов критической информационной инфраструктуры. / Ср /	2	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.5, Л2.1, Л2.4, Л2.5
7.5	Мониторинг и аудит безопасности объектов критической информационной инфраструктуры. / Ср /	2	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.5, Л2.1, Л2.4, Л2.5
7.6	Методы и средства защиты объектов критической информационной инфраструктуры. / Ср /	2	2	ПК-2	Л1.1, Л1.2, Л1.3, Л1.5, Л2.1, Л2.4, Л2.5
7.7	Выполнение заданий с использованием LibreOffice. / Ср /	2	34	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
Раздел 8. Организация аудита информационной безопасности					
№	**Наименование темы / Вид занятия**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**
8.1	Аудит информационной безопасности. Виды аудита, предназначение и особенности проведения Аудита ИБ. Риск-менеджмент (модель угроз). -- / Лек /	2	2	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
8.2	Методы и инструменты для анализа рисков информационных систем. Создание модели угроз на предприятии. / Пр /	2	8	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
8.3	Мониторинг и аудит безопасности информационных систем. / Ср /	2	8	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
8.4	Мониторинг и аудит безопасности информационных систем. / Ср /	2	4	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
8.5	Выполнение заданий с использованием LibreOffice. / Ср /	2	42	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5
Раздел 9. Промежуточная аттестация					
№	**Наименование темы / Вид занятия**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**
9.1	/ Экзамен /	2	36	ПК-2	Л1.1, Л1.2, Л1.3, Л1.4, Л1.5, Л2.1, Л2.2, Л2.3, Л2.4, Л2.5

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	Руденков Н. А., Пролетарский А. В., Смирнова Е. В., Суровов А. М.	Технологии защиты информации в компьютерных сетях: учебное пособие	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	https://biblioclub.ru/index.php?page=book&id=428820 неограниченный доступ для зарегистрированных пользователей
Л1.2	Ковалев Д. В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов-на-Дону: Южный федеральный университет, 2016	https://biblioclub.ru/index.php?page=book&id=493175 неограниченный доступ для зарегистрированных пользователей
Л1.3	Катанова, Т. Н., Галкина, Л. С., Жданов, Р. А.	Информационная безопасность: лабораторный практикум	Пермь: Пермский государственный гуманитарно-педагогический университет, 2018	https://www.iprbookshop.ru/86357.html неограниченный доступ для зарегистрированных пользователей
Л1.4	Шилов, А. К.	Управление информационной безопасностью: учебное пособие	Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2018	https://www.iprbookshop.ru/87643.html неограниченный доступ для зарегистрированных пользователей
Л1.5	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	https://www.iprbookshop.ru/87995.html неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.1		Вестник Института законодательства и правовой информации имени М.М. Сперанского: журнал	Иркутск: Институт законодательства и правовой информации, 2017	https://biblioclub.ru/index.php?page=book&id=457912 неограниченный доступ для зарегистрированных пользователей
Л2.2	Рогозин, В. Ю., Галушкин, И. Б., Новиков, В. К., Вепрев, С. Б.	Основы информационной безопасности: учебник для студентов вузов, обучающихся по направлению подготовки «правовое обеспечение национальной безопасности»	Москва: ЮНИТИ-ДАНА, 2017	https://www.iprbookshop.ru/72444.html неограниченный доступ для зарегистрированных пользователей
Л2.3	Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н.	Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: учебно-методическое пособие к прохождению производственной практики: учебно-методическое пособие	Йошкар-Ола: Поволжский государственный технологический университет, 2019	https://biblioclub.ru/index.php?page=book&id=562246 неограниченный доступ для зарегистрированных пользователей
Л2.4		БИТ. Бизнес & Информационные технологии: журнал	Москва: Положевец и партнеры, 2019	https://biblioclub.ru/index.php?page=book&id=562409 неограниченный доступ для зарегистрированных пользователей

	Авторы,	Заглавие	Издательство, год	Колич-во
Л2.5	Суворова, Г. М.	Информационная безопасность: учебное пособие	Саратов: Вузовское образование, 2019	https://www.iprbookshop.ru/86938.html неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Информационная справочная система "КонсультантПлюс"
База данных Федеральной службы по техническому и экспортному контролю (ФСТЭК России) https://fstec.ru/
База данных действующих стандартов по направлению "Информационная Безопасность" https://www.gost.ru/portal/gost/home/standarts/InformationSecurity

5.4. Перечень программного обеспечения

LibreOffice, Kali Linux

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

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:
- столы, стулья;
- персональный компьютер / ноутбук (переносной);
- проектор;
- экран / интерактивная доска.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

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

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ПК-2: Способен управлять ИТ-инфраструктурой предприятия с учетом требований обеспечения информационной безопасности			
Знать принципы работы современных технологий обеспечения информационной безопасности при решении задач профессиональной деятельности	Описывает способы решения стандартных задач профессиональной деятельности в области информационной безопасности при формировании системы защиты информации при ответе на вопросы	Полный, развёрнутый ответ на поставленный вопрос, изложение материала при ответе – грамотное и логически стройное	Опрос (вопросы 1-57) Вопросы к зачету (вопросы 1-22) Вопросы к экзамену (вопросы 1-19)
Уметь решать стандартные задачи профессиональной деятельности с учетом требований информационной безопасности	Анализирует состояние системы защиты информации, выявляет ее уязвимые места и определяет направления ее совершенствования при выполнении практико-ориентированного задания	Полнота и правильность решения практико-ориентированного задания задания	Практико-ориентированные задания (задания 1-8) Практико-ориентированные задания к зачету (задания 1-24) Практико-ориентированные задания к экзамену (задания 1-23)
Владеть навыками использования способов и средств защиты информации при решении задач профессиональной деятельности	Использует методы и средства защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России и ФСТЭК России при выполнении практико-ориентированного задания	Обоснованность и правильность обращения к нормативным источникам, методам и средствам при выполнении практико-ориентированного задания	Практико-ориентированные задания (задания 1-8) Практико-ориентированные задания к зачету (задания 1-24) Практико-ориентированные задания к экзамену (задания 1-23)

1.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале:

84-100 баллов (оценка «отлично»)

67-83 баллов (оценка «хорошо»)

50-66 баллов (оценка «удовлетворительно»)

0-49 баллов (оценка «неудовлетворительно»)

50-100 баллов (зачтено)

0-49 баллов (не зачтено)

2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Вопросы к зачету

1. Понятие и виды информации. Классификация в зависимости от категории доступа. Сведения конфиденциального характера. Виды защищаемой информации.
2. Понятие, предназначение, виды и классификация государственных информационных систем.
3. Основное законодательство в области информационной безопасности в РФ. Доктрина информационной безопасности РФ.
4. Основные модели информационной безопасности: особенности, отличия.
5. Организационные уровни защиты информации: Средства безопасности законодательного уровня.
6. Организационные уровни защиты информации: Административный уровень информационной безопасности.
7. Организационные уровни защиты информации: Средства безопасности процедурного уровня.
8. Организационные уровни защиты информации: Средства безопасности технического уровня.
9. Угрозы. Виды и классификация угроз.
10. Уязвимости. Виды уязвимостей, поиск и выявление уязвимостей.
11. Атака. Основные виды компьютерных атак, их классификация.
12. Активные и пассивные атаки. Виды реализации атак.
13. Модель построения атаки Cyber Kill Chain: предназначение, состав, содержание основных этапов.
14. Матрица MITRE ATT&CK: предназначение, состав, основные тактики.
15. Компьютерные вирусы: определение, основная классификация, виды компьютерных вирусов.
16. Основной «жизненный» цикл компьютерных вирусов, признаки их распространения и проявления.
17. Антивирусные программы: типы, состав основных и дополнительных модулей, принцип работы. Основные методики обнаружения и защиты от компьютерных вирусов.
18. Методики противодействия антивирусным программам.
19. Парольная защита. Парольные методы аутентификации пользователей. Основные факторы, влияющие на криптостойкость пароля.
20. Идентификация (пользователей) и аутентификация. Двусторонняя аутентификация. Авторизация.
21. Виды парольных атак для подбора пароля.
22. Рекомендации ФСТЭК России по практической реализации парольных систем.

Практико-ориентированные задания к зачету

1. Разработка концепции и программы обеспечения информационной безопасности в рамках национальной безопасности РФ.
2. Выбор метода исследования нормативно-правовой базы функционирования систем защиты информации.
3. Получение первичной информации о правовых актах, регулирующих информационную безопасность в России.
4. Обработка первичной информации и разработка предложений по совершенствованию нормативно-правовой базы.
5. Изучение особенностей защиты программного обеспечения с помощью авторского права.
6. Разработка метода исследования случаев нарушения авторских прав на программное обеспечение.
7. Получение первичной информации об известных нарушениях авторских прав на программное обеспечение.
8. Обработка первичной информации и разработка предложений по усилению защиты программного обеспечения.
9. Разработка концепции и программы организации работы с конфиденциальной информацией и гостайной.
10. Выбор метода исследования требований к хранению, обработке и транспортировке конфиденциальной информации.

11. Получение первичной информации об особенностях работы с конфиденциальной информацией в различных организациях.
12. Обработка первичной информации и разработка рекомендаций по организации работы с конфиденциальной информацией.
13. Разработка модели угроз утечки информации по техническим каналам.
14. Выбор метода исследования физических основ возникновения технических каналов утечки информации.
15. Получение первичной информации об известных случаях утечки информации по техническим каналам.
16. Обработка первичной информации и разработка предложений по предотвращению утечки информации по техническим каналам.
17. Разработка модели рисков, связанных с утечками информации из-за ПЭМИ и наводок.
18. Выбор метода исследования эффективности средств защиты от ПЭМИ и наводок.
19. Получение первичной информации об имеющихся на рынке средствах защиты от ПЭМИ и наводок.
20. Обработка первичной информации и разработка рекомендаций по выбору оптимальных средств защиты от ПЭМИ и наводок.
21. Разработка модели рисков, связанных с утечками информации из-за хакерских атак и вмешательства в процесс передачи данных.
22. Выбор метода исследования принципов функционирования симметричных и асимметричных криптосистем.
23. Получение первичной информации об имеющихся на рынке криптосистемах и их эффективности.
24. Обработка первичной информации и разработка рекомендаций по выбору оптимальных криптосистем для защиты информации.

Зачетное задание включает 2 теоретических вопроса (раздел «Вопросы к зачету») и 1 практико-ориентированное задание (формируется из перечня заданий, представленных в разделе «Практико-ориентированные задания к зачету»).

Критерии оценивания:
Максимальное количество баллов за зачетное задание – 100 (30 баллов максимально за каждый теоретический вопрос, 40 баллов максимально за практико-ориентированное задание).

Критерии оценивания одного теоретического вопроса:
– 25-30 баллов выставляется студенту, если изложенный материал фактически верен, продемонстрированы глубокие исчерпывающие знания в объеме пройденной программы в соответствии с поставленными программой курса целями и задачами обучения, изложение материала при ответе - грамотное и логически стройное;
– 20-24 баллов выставляется студенту, если продемонстрированы твердые и достаточно полные знания в объеме пройденной программы дисциплины в соответствии с целями обучения; материал изложен достаточно полно с отдельными логическими и стилистическими погрешностями;
– 15-19 баллов выставляется студенту, если продемонстрированы твердые знания в объеме пройденного курса в соответствие с целями обучения, ответ содержит отдельные ошибки, уверенно исправленные после дополнительных вопросов;
– 0-14 балла выставляется студенту, если ответы не связаны с вопросами, допущены грубые ошибки в ответе, продемонстрированы непонимание сущности излагаемого вопроса, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Критерии оценивания практико-ориентированного задания:
– 35-40 баллов выставляется, если задание решено полностью, в представленном решении обоснованно получены правильные ответы.
– 25-34 балла выставляется, если задание решено полностью, но при ответе допущены незначительные ошибки.
– 11-24 балла выставляется, если задание решено частично.

– 0-10 баллов выставляется, если решение неверно или отсутствует.

Итоговый результат формируется из суммы набранных баллов за выполнение зачетного задания и соответствует шкале:
– 50-100 баллов (зачтено);
– 0-49 баллов (не зачтено).

Вопросы к экзамену

1. Понятие и виды информации. Виды защищаемой информации. Основные подходы в защите информации.
2. Угрозы. Виды и классификация угроз.
3. Уязвимости. Виды уязвимостей, поиск и выявление уязвимостей.
4. Атака. Основные виды компьютерных атак, их классификация.
5. Активные и пассивные атаки. Виды реализации атак.
6. Модель построения атаки Cyber Kill Chain. Матрица MITRE ATT&CK. Предназначение, состав, содержание основных этапов (тактик).
7. Компьютерные вирусы. Виды компьютерных вирусов. Методики обнаружения и защиты от компьютерных вирусов.
8. Парольная защита. Парольные методы аутентификации пользователей. Основные факторы, влияющие на криптостойкость пароля.
9. Способы идентификация и аутентификации (пользователей). Двухфакторная и многофакторная аутентификация. Способы обхода аутентификации.
10. Виды и способы реализации парольных атак.
11. Персональные данные (ПДн). Виды персональных данных. Способы обработки персональных данных.
12. Защита персональных данных (ПДн). Урони защищенности ПДн.
13. Криптография. Криптографические ключи и алгоритмы. Виды шифрования.
14. Электронная подпись (ЭП). Виды и предназначение ЭП. Принцип функционирования, порядок выдачи ЭП.
15. Критическая информационная инфраструктура (КИИ) — объекты, субъекты, критерии, определяющие принадлежность к КИИ.
16. Содержание и порядок этапов категорирования КИИ. Критерии и показатели значимости.
17. ГосСОПКА. Предназначение, решаемые задачи и направление деятельности.
18. Основные программно-аппаратные системы ГосСОПКА. Состав, предназначение.
19. SIEM-система. Предназначение, применение, основные решаемые задачи.

Практико-ориентированные задания к экзамену

1. Проанализируйте законодательство, регулирующее лицензирование в области защиты информации.
2. Опишите процедуру получения лицензии на оказание услуг в области защиты информации.
3. Разработайте план действий по подготовке и подаче документов для лицензирования.
4. Опишите процедуру получения лицензии на оказание услуг в области защиты информации.
5. Разработайте план действий по подготовке и подаче документов для лицензирования.
6. Определите сущность и содержание коммерческой тайны в соответствии с законодательством.
7. Опишите права и обязанности сторон при охране коммерческой тайны.
8. Разработайте процедуру определения списка сведений, составляющих коммерческую тайну.
9. Опишите права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные.
10. Разработайте процедуру защиты персональных данных в организации.
11. Разработайте положение об обработке и защите персональных данных в организации.
12. Опишите организационные мероприятия, необходимые для обеспечения защиты информации.

13. Разработайте процедуру контроля состояния защиты информации.
14. Разработайте процедуру разработки политики безопасности предприятия.
15. Опишите требования к защите персональных данных в электронных коммуникациях.
16. Разработайте рекомендации по обеспечению безопасности передачи персональных данных через Интернет.
17. Разработайте рекомендации по защите персональных данных в социальных сетях и мобильных приложениях.
18. Опишите требования к защите персональных данных в облачных службах и больших данных.
19. Разработайте рекомендации по обеспечению безопасности персональных данных в облачных службах и больших данных.
20. Опишите требования к защите персональных данных в искусственном интеллекте, биометрии и интернете вещей.
21. Разработайте рекомендации по обеспечению безопасности персональных данных в искусственном интеллекте, биометрии и интернете вещей.
22. Опишите требования к защите персональных данных в видеонаблюдении.
23. Разработайте рекомендации по защите персональных данных в видеонаблюдении.

Экзаменационное задание включает 2 теоретических вопроса (раздел «Вопросы к экзамену») и 1 практико-ориентированное задание (формируется из перечня заданий, представленных в разделе «Практико-ориентированные задания к экзамену»).

Критерии оценивания:
Максимальное количество баллов за экзаменационное задание – 100 (30 баллов максимально за каждый теоретический вопрос, 40 баллов максимально за практико-ориентированное задание).

Критерии оценивания одного теоретического вопроса:
– 25-30 баллов выставляется студенту, если изложенный материал фактически верен, продемонстрированы глубокие исчерпывающие знания в объеме пройденной программы в соответствии с поставленными программой курса целями и задачами обучения, изложение материала при ответе - грамотное и логически стройное;
– 20-24 баллов выставляется студенту, если продемонстрированы твердые и достаточно полные знания в объеме пройденной программы дисциплины в соответствии с целями обучения; материал изложен достаточно полно с отдельными логическими и стилистическими погрешностями;
– 15-19 баллов выставляется студенту, если продемонстрированы твердые знания в объеме пройденного курса в соответствие с целями обучения, ответ содержит отдельные ошибки, уверенно исправленные после дополнительных вопросов;
– 0-14 балла выставляется студенту, если ответы не связаны с вопросами, допущены грубые ошибки в ответе, продемонстрированы непонимание сущности излагаемого вопроса, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Критерии оценивания практико-ориентированного задания:
– 35-40 баллов выставляется, если задание решено полностью, в представленном решении обоснованно получены правильные ответы.
– 25-34 балла выставляется, если задание решено полностью, но при ответе допущены незначительные ошибки.
– 11-24 балла выставляется, если задание решено частично.
– 0-10 баллов выставляется, если решение неверно или отсутствует.

Итоговый результат формируется из суммы набранных баллов за выполнение зачетного задания и соответствует шкале:
– 84-100 баллов (оценка «отлично»)
– 67-83 баллов (оценка «хорошо»)

– 50-66 баллов (оценка «удовлетворительно»)
– 0-49 баллов (оценка «неудовлетворительно»)

Опрос

Вопросы для опроса 1 семестра:

1. Информация как объект правового регулирования.
2. Структура законодательства РФ в области информационной безопасности и защиты информации.
3. Основные цели и методы обеспечения ИБ РФ. Источники и виды угроз ИБ РФ.
4. Основные направления обеспечения информационной безопасности и защиты информации в РФ.
5. Структура организационной защиты информации.
6. Виды информации, защищаемой законодательством РФ.
7. Перечень сведений конфиденциального характера.
8. Организация работы со сведениями, отнесенными к конфиденциальной информации.
9. Правовой режим защиты конфиденциальной информации.
10. Угрозы утечки информации по техническим каналам.
11. Формы защищаемой информации.
12. Основные объекты защиты информации.
13. Классификация технических каналов утечки информации.
14. Технические мероприятия по защите информации от утечки по техническим каналам.
15. Организационные мероприятия по защите информации от утечки по техническим каналам.
16. Классификации угроз безопасности информации в информационных системах.
17. Требования к организации защиты информации в информационной системе.
18. Формирование требований к защите информации в информационной системе.
19. Обеспечение защиты информации в ходе эксплуатации информационной системы.
20. Требования к мерам защиты информации, содержащейся в информационной системе.
21. Определение класса защищенности информационной системы.
22. Лицензирование в области защиты информации.
23. Структура системы государственного лицензирования.
24. Порядок проведения лицензирования.
25. Основные лицензионные требования и условия в области защиты информации.
26. Перечень видов деятельности в области защиты информации, подлежащих лицензированию.
27. Структура системы сертификации.
28. Порядок проведения сертификации средств защиты информации.
29. Сертификационные испытания средств защиты информации.

Вопросы для опроса 2 семестра:

30. Порядок отнесения информации к информации, составляющей коммерческую тайну, и ее предоставление.
31. Понятие коммерческой тайны. Правовое обеспечение защиты коммерческой тайны.
32. Сведения, составляющие коммерческую тайну. Сведения, которые не могут составлять коммерческую тайну.
33. Права обладателя коммерческой тайны.
34. Организация защиты информации на предприятии.
35. Обеспечение сохранности документов, дел и изданий.
36. Обязанности лиц, допущенных к сведениям, составляющих коммерческую тайну.
37. Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.
38. Обязанности персонала организации по сохранению коммерческой тайны.
39. Политика безопасности предприятия как основа организационного управления защитой информации.
40. Права и обязанности работника и работодателя по защите конфиденциальной информации.
41. Ответственность за нарушение конфиденциальности информации.
42. Права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные.

43. Организация защиты персональных данных в организации.
44. Планирование мероприятий по организационной защите информации на предприятии.
45. Структура и основное содержание плана мероприятий по защите конфиденциальной информации.
46. Организация аналитической работы в области защиты информации на предприятии.
47. Основные объекты и формы контроля за состоянием защиты информации.
48. Основные задачи и методы контроля.
49. Основные направления аналитической работы.
50. Организация аудита информационной безопасности предприятия.
51. Функции аналитического подразделения в области защиты информации на предприятии.
52. Основные этапы аналитической работы в области защиты информации на предприятии.
53. Содержание и основные виды аналитических отчетов.
54. Классификация методов анализа информации.
55. Компьютерные преступления в электронной коммерции.
56. Информационная безопасность в электронной коммерции.
57. Юридическая ответственность за нарушение правовых норм защиты информации.

Критерии оценивания*:*
Максимальное количество баллов, которое обучающийся может набрать за семестр – 20 баллов (за 20 ответов).
Ответ на вопрос оценивается:
– 1 балл – правильный и полный ответ;
– 0 баллов – неправильный ответ или ответ не представлен.

Практико-ориентированные задания

Практико-ориентированные задания для 1 семестра:

Задание 1.
Работа с ИСС "Консультант Плюс": Базовые свойства безопасности информации. Нормативно-правовая база функционирования систем защиты информации. Правовая защита программного обеспечения авторским правом. Компьютерные преступления и особенности их расследования.
Задание 2
Работа с ИСС «КонсультантПлюс», БД Федеральной службы по техническому и экспортному контролю (ФСТЭК России) https://fstec.ru/: Формы защищаемой информации. Объекты защиты. Физические основы возникновения ТКУИ. Классификация ТСР.

Задание 3.
Работа с ИСС «КонсультантПлюс», БД Федеральной службы по техническому и экспортному контролю (ФСТЭК России) https://fstec.ru/: Построение типовых моделей угроз безопасности информации, обрабатываемой в информационных системах.

Задание 4.
Система шифрования Цезаря. Шифры перестановки.
1. Реализовать систему шифрования Цезаря. Система шифрования Цезаря, в котором каждый символ в открытом тексте сдвигается на определенное число позиций вперед или назад. Реализовать функции шифрования и дешифрования текста с использованием системы шифрования Цезаря.
2. Реализовать шифры перестановки, в которых порядок символов в открытом тексте меняется согласно некоторой функции. Реализовать функции шифрования и дешифрования текста с использованием шифров перестановки.
3. Реализовать систему шифрования Цезаря с ключом.
4. Реализовать функции шифрования и дешифрования текста с использованием системы шифрования Цезаря с ключом.

Практико-ориентированные задания для 1 семестра:

Задание 5.

Реализация двустороннего обмена ключевой информацией. Понятие и назначение центра распределения ключей. Требования Диффи и Хеллмана.
Реализовать функции для генерации простых чисел и вычисления наибольшего общего делителя.

1. Реализовать функции для генерации ключевой пары и обмена ключевой информацией с использованием протокола Диффи-Хеллмана.
2. Реализовать тесты для функций генерации ключевой пары и обмена ключевой информацией.
3. Реализовать тесты для функций генерации ключевой пары и обмена ключевой информацией.

Задание 6.
Алгоритм шифрования RSA. Процесс формирования ключевой пары получателем, шифрование и дешифрование сообщений в криптосистеме RSA.

1. Реализовать функции для генерации простых чисел, вычисления наибольшего общего делителя, нахождения обратного элемента по модулю.
2. Реализовать функции для генерации ключевой пары и шифрования/дешифрования сообщений с использованием алгоритма RSA.
3. Реализовать тесты для функций генерации ключевой пары и шифрования/дешифрования сообщений.

Задание 7.
Формирование перечня сведений, составляющих коммерческую тайну.

1. Выберите вымышленную компанию, для которой будете формировать перечень сведений, составляющих коммерческую тайну.
2. Опишите виды сведений, которые могут составлять коммерческую тайну для выбранной компании.
3. Составьте перечень сведений, составляющих коммерческую тайну, для выбранной компании.
4. Оформите результаты в виде отчета

Задание 8.
Разработка политики безопасности предприятия.

1. Определите цели и задачи политики безопасности предприятия.
2. Опишите меры по защите информации, собственности и персонала предприятия.
3. Разработайте процедуры ответа на угрозы безопасности предприятия.
4. Оформите результаты в виде документа политики безопасности предприятия.

Критерии оценивания:
Максимальное количество баллов, которое обучающийся может набрать за семестр – 80 баллов (за 4 задания в семестр).
Каждое задание оценивается:

- 20 баллов. – задание выполнено верно;
- 19-14 баллов. – при выполнении задания были допущены неточности, не влияющие на результат;
- 13-6 баллов. – при выполнении задания были допущены ошибки;
- 5- 1 баллов. – при выполнении задания были допущены существенные ошибки;
- 0 баллов. – задание не выполнено.

3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.
Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.
Промежуточная аттестация проводится в форме зачета, экзамена.
Зачет проводится по расписанию промежуточной аттестации в устной форме. Количество вопросов в зачетном задании – 3 (2 теоретических, 1 практико-ориентированное задание). Результаты аттестации

заносятся в ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.
Экзамен проводится по расписанию промежуточной аттестации в устной форме. Количество вопросов в экзаменационном задании – 3 (2 теоретических, 1 практико-ориентированное задание). Результаты аттестации заносятся в ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:
- лекции;
- практические занятия.

В ходе лекционных занятий рассматриваются основные понятия в области информационной безопасности и защиты информации, методы обнаружения и организации противодействия атак на информационные сети, требования по защите конфиденциальной информации, даются рекомендации для самостоятельной работы и подготовки к практическим занятиям.

В ходе практических занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки решения задач по защите информационных объектов.

При подготовке к практическим занятиям каждый студент должен:
- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- ознакомиться с описанием практической работы;

В процессе подготовки к практическим занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на лекциях и практических занятиях, должны быть изучены студентами в ходе самостоятельной работы. В ходе самостоятельной работы каждый студент обязан прочитать основную и, по возможности, дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных источников. Выделить непонятные термины и найти их значение в энциклопедических словарях.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.