МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

04.12.2025 г.

протокол № 12

Зав. кафедрой Банных С.Г.

Утверждена
Советом по учебно-методическим вопросам и качеству образования

16 декабря 2025 г.

протокол № 4

Председатель _____ Карх Д.А.
(подпись)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины	Информационная политика организации
Направление подготовки	38.04.01 Экономика
Профиль	Экономическая безопасность и управление рисками
Форма обучения	очная
Год набора	2026

Разработана:
Профессор, д.ф.н.
Матвеева А.И.

Екатеринбург
2025 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Рабочая программа дисциплины является частью основной профессиональной образовательной программы высшего образования - программы магистратуры, разработанной в соответствии с ФГОС ВО

ФГОС ВО	Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 38.04.01 Экономика (приказ Минобрнауки России от 11.08.2020 г. № 939)

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

- изучение принципов обеспечения информационной безопасности государства, подходов к анализу угроз его информационной инфраструктуры и освоение

дисциплинарных компетенций для решения задач защиты информации в информационных системах, а также формирование фундаментальных знаний в области информационной безопасности организации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к части, формируемой участниками образовательных отношений.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Промежуточная аттестация	Часов					З.е.
	Всего за семестр	Контактная работа .(по уч.зан.)			Самостоятельная работа в том числе подготовка контрольных и курсовых	
		Всего	Лекции	Практические занятия, включая курсовое проектирование		
Семестр 3						
Зачет с оценкой	144	24	8	16	120	4

4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

В результате освоения ОПОП у выпускника должны быть сформированы компетенции, установленные в соответствии ФГОС ВО.

Шифр и наименование компетенции	Индикаторы достижения компетенций
проектно-экономический	

ПК-2 Оценка эффективности управления рисками в организации, в т.ч. в кредитной организации, и представление результатов органам управления организации	ИД-1.ПК-2 Знать: Законодательство Российской Федерации по виду деятельности организации и требования (рекомендации) области управления рисками; Международные и российские стандарты по риск-менеджменту и риск -ориентированному управлению организацией; Корпоративные финансы, теория вероятности и математическая статистика, корпоративное управление, поведенческая экономика, нейроэкономика и теория принятия решений; Перечень заинтересованных сторон; Организацию управленческой отчетности организации, отдельных бизнес-процессов, проектов, решений; Цели организации, цели и задачи бизнес-процессов, цели ключевых управленческих решений; Организационную структуру организации; Органы управления организации; Подходы к управлению, методы и инструменты управления рисками, в том числе оценки рисков, включая идентификацию и анализ влияния рисков на цели организации и ключевые показатели деятельности, приоритизации рисков, определения критериев существенности; Состав, форму и порядок формирования отчетности с учетом рисков; Модели зрелости в области управления рисками; Критерии оценки уровня зрелости методики управления рисками; Методы формирования дорожной карты внедрения риск-ориентированного подхода к управлению организацией; Программное обеспечение в области риск-ориентированного управления организацией, оценки влияния рисков на цели организации; Подходы к коммуникации и доведению информации до исполнительных органов и совета директоров; Подходы к коммуникации и доведению информации до исполнительных органов и совета директоров; Нормы профессиональной этики; Профессиональные сообщества; Иностранный язык в объеме, необходимом для выполнения трудовой функции; Основы осуществления защиты персональных данных; Основы работы в операционных системах; Принципы соблюдения информационной безопасности, сохранения конфиденциальности данных.

ПК-2 Оценка эффективности управления рисками в организации, в т.ч. в кредитной организации, и представление результатов органам управления организации	ИД-2.ПК-2 Уметь: Определять заинтересованные стороны в реализации риск-ориентированного управления в организации на уровне акционеров, совета директоров, партнеров, руководства организации; Проводить интервью с заинтересованными сторонами, изучение требований (рекомендаций) в отношении внедрения риск-ориентированного управления организацией или управления рисками; Изучать существующие требования (рекомендации) в отношении внедрения риск-ориентированного управления организацией или управления рисками; Сравнивать и выбирать существующие модели зрелости управления рисками и критерии оценки уровня зрелости методики управления рисками; Представлять заинтересованным сторонам, обсуждать и согласовывать результаты оценки уровня зрелости, рекомендации по внедрению риск-ориентированного управления организацией; Формировать и представлять материалы о достижениях организации в области управления рисками в рамках профессиональных сообществ; Изучать лучшую практику внедрения риск-ориентированного управления на предмет применения в организации; Создавать и воспроизводить видеоролики, презентации, слайд-шоу, медиафайлы и итоговую продукцию из исходных аудиокомпонентов, визуальных и мультимедийных компонентов; Применять подходы безопасной работы в информационно-телекоммуникационной сети "Интернет" (защита персональных данных, антивирусная защита, информационная гигиена); Управлять размещением цифровой информации, в том числе в дисковых хранилищах локальной и глобальной компьютерной сети; Формировать медиатеки для структурированного хранения и каталогизации цифровой информации.
	ИД-3.ПК-2 Иметь практический опыт: Определения заинтересованных сторон в реализации риск-ориентированного управления в организации на уровне акционеров, совета директоров, партнеров, руководства организации; Проведения интервью с заинтересованными сторонами, изучение требований (рекомендаций) в отношении внедрения риск-ориентированного управления организацией или управления рисками Выбора подхода и критериев оценки уровня зрелости методики управления рисками Согласования и представления результатов оценки уровня зрелости, рекомендаций по внедрению риск-ориентированного управления организацией заинтересованным сторонам Обмена знаниями в области управления рисками в рамках профессиональных сообществ, изучение лучшей практики внедрения риск-ориентированного управления в организациях для дальнейшей оценки уровня зрелости.
аналитический	

ПК-1 Раскрытие информации о рисках организации, в т.ч. кредитной организации, в отчетах для внешних сторон, связанных с требованиями регуляторов и достижением стратегических целей или принимаемыми стратегическими решениями	ИД-1.ПК-1 Знать: Законодательство Российской Федерации по виду деятельности организации и требования (рекомендации) области управления рисками; Международные и российские стандарты по риск-менеджменту и риск -ориентированному управлению организацией; Перечень заинтересованных сторон; Организацию внешней и внутренней отчетности организации, бизнес-подразделений; Состав, форму и порядок формирования отчетности с учетом рисков; Подходы к коммуникации и доведению информации до исполнительных органов и совета директоров; Нормы профессиональной этики; Иностранный язык в объеме, необходимом для выполнения трудовой функции; Защиту персональных данных; Основы работы в операционных системах; Принципы соблюдения информационной безопасности, сохранения конфиденциальности данных.
	ИД-2.ПК-1 Уметь: Определять заинтересованные стороны в реализации риск-ориентированного управления в организации на уровне акционеров, совета директоров, партнеров, руководства организации; Организовывать работы по раскрытию информации о рисках в отчетах для внешних сторон, связанных с требованиями регуляторов и достижением стратегических целей или с принимаемыми стратегическими решениями; Выстраивать коммуникации с заинтересованными сторонами; Создавать и воспроизводить видеоролики, презентации, слайд-шоу, медиафайлы и итоговую продукцию из исходных аудиокомпонентов, визуальных и мультимедийных компонентов; Применять подходы безопасной работы в информационно-телекоммуникационной сети "Интернет" (защита персональных данных, антивирусная защита, информационная гигиена); Управлять размещением цифровой информации, в том числе в дисковых хранилищах локальной и глобальной компьютерной сети; Формировать медиатеки для структурированного хранения и каталогизации цифровой информации.
	ИД-3.ПК-1 Иметь практический опыт: Определения заинтересованных сторон на уровне акционеров, совета директоров, партнеров, руководства организации для раскрытия информации о рисках; Организации работы по раскрытию информации о рисках в отчетах для внешних сторон, связанных с требованиями регуляторов и достижением стратегических целей или с принимаемыми стратегическими решениями; Создания каналов коммуникации для передачи и эскалации информации в области управления рисками с акционерами, советом директоров, партнерами, руководством организации.

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов

	Наименование темы	Всего часов	Контактная работа .(по уч.зан.)			Самост. работа	Контроль самостоятельной работы
			Лекции	Лабораторные	Практические занятия		
Семестр 3		144					
Тема 1.	Теоретические аспекты информационной безопасности экономических систем (ПК-1)	17	1		2	14	
Тема 2.	Понятие информационных угроз и их виды (ПК-1, ПК-2)	23	1		2	20	
Тема 3.	Государственное регулирование ИБ (ПК-1)	28	1		2	25	
Тема 4.	Подходы, принципы, методы и средства обеспечения безопасности (ПК-1, ПК-2)	25	1		2	22	
Тема 5.	Организация системы защиты информации (ПК-1, ПК-2)	23	2		4	17	
Тема 6.	Менеджмент и аудит систем ИБ (ПК-2)	28	2		4	22	

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочного средства	Описание оценочного средства	Критерии оценивания
Текущий контроль (Приложение 4)			
Тема 1 Тема 2	контрольная работа №1 (Приложение 4)	Контрольная работа состоит из теста в котором 25 вопросов. 16 вопросов закрытого типа. В каждом вопросе 3 правильных ответа. 9 вопросов открытого типа.	49 и менее неудовлетворительно, 69% - 50% удовлетворительно, 84% - 70% хорошо, 100% - 85% отлично
Тема 3	Контрольная работа №2 (Приложение 4)	Контрольная работа состоит из теста в котором 20 вопросов. Из низ 12 вопросов закрытых (в каждом вопросе 4 ответа и только один правильный). 12 вопросов открытого типа.	49 и менее неудовлетворительно, 69% - 50% удовлетворительно, 84% - 70% хорошо, 100% - 85% отлично
Тема 4	Контрольная работа №3 (Приложение 4)	Контрольная работа состоит из теста в котором 15 вопросов. 10 вопросов закрытого типа (в каждом вопросе 4 варианта и только один правильный) 10 вопросов открытого типа.	49 и менее неудовлетворительно, 69% - 50% удовлетворительно, 84% - 70% хорошо, 100% - 85% отлично

Тема 5	контрольная работа № 4 (Приложение 4)	Контрольная работа состоит из теста в котором 15 вопросов. 10 вопросов закрытого типа (в каждом вопросе 4 варианта и только один правильный) 10 вопросов открытого типа.	49 и менее неудовлетворительно, 69% - 50% удовлетворительно, 84% - 70% хорошо, 100% - 85% отлично
Тема 6	контрольная работа №5 (Приложение 4)	Контрольная работа состоит из теста в котором 15 вопросов. 3 вопроса закрытого типа (в каждом вопросе 4 варианта и только один правильный) 12 вопросов открытого типа.	49 и менее неудовлетворительно, 69% - 50% удовлетворительно, 84% - 70% хорошо, 100% - 85% отлично
Промежуточная аттестация (Приложение 5)			
3 семестр (ЗаО)	Итоговая контрольная работа в виде теста (Приложение № 5)	Тест состоит из 40 вопросов. 10 вопросов закрытых. В каждом вопросе по четыре варианта ответа и только один правильный. 30 вопросов открытых	49 и менее неудовлетворительно, 69% - 50% удовлетворительно, 84% - 70% хорошо, 100% - 85% отлично

ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Показатель оценки освоения ОПОП формируется на основе объединения текущего контроля и промежуточной аттестации обучающегося.

Показатель рейтинга по каждой дисциплине выражается в процентах, который показывает уровень подготовки студента.

Текущий контроль. Используется 100-балльная система оценивания. Оценка работы студента в течении семестра осуществляется преподавателем в соответствии с разработанной им системой оценки учебных достижений в процессе обучения по данной дисциплине.

В рабочих программах дисциплин и практик закреплены виды текущего контроля, планируемые результаты контрольных мероприятий и критерии оценки учебный достижений.

В течение семестра преподавателем проводится не менее 3-х контрольных мероприятий, по оценке деятельности студента. Если посещения занятий по дисциплине включены в рейтинг, то данный показатель составляет не более 20% от максимального количества баллов по дисциплине.

Промежуточная аттестация. Используется 5-балльная система оценивания. Оценка работы студента по окончанию дисциплины (части дисциплины) осуществляется преподавателем в соответствии с разработанной им системой оценки достижений студента в процессе обучения по данной дисциплине. Промежуточная аттестация также проводится по окончанию формирования компетенций.

Порядок перевода рейтинга, предусмотренных системой оценивания, по дисциплине, в пятибалльную систему.

Высокий уровень – 100% - 70% - отлично, хорошо.

Средний уровень – 69% - 50% - удовлетворительно.

Показатель оценки	По 5-балльной системе	Характеристика показателя
100% - 85%	отлично	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на высоком уровне
84% - 70%	хорошо	обладают теоретическими знаниями в полном объеме, понимают, самостоятельно умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Могут быть допущены недочеты, исправленные студентом самостоятельно в процессе работы (ответа и т.д.)
69% - 50%	удовлетворительно	обладают общими теоретическими знаниями, умеют применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов на среднем уровне. Допускаются ошибки, которые студент затрудняется исправить самостоятельно.
49 % и менее	неудовлетворительно	обладают не полным объемом общих теоретическими знаниями, не умеют самостоятельно применять, исследовать, идентифицировать, анализировать, систематизировать, распределять по категориям, рассчитать показатели, классифицировать, разрабатывать модели, алгоритмизировать, управлять, организовать, планировать процессы исследования, осуществлять оценку результатов. Не сформированы умения и навыки для решения профессиональных задач
100% - 50%	зачтено	характеристика показателя соответствует «отлично», «хорошо», «удовлетворительно»
49 % и менее	не зачтено	характеристика показателя соответствует «неудовлетворительно»

7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

7.1. Содержание лекций

Тема 1. Теоретические аспекты информационной безопасности экономических систем (ПК-1)

Информационное общество. Информационное пространство. Информационная война и информационное противоборство. Информационная преступность. Угрозы безопасности информации. Информационная безопасность (ИБ). Политика безопасности. Объекты и субъекты обеспечения ИБ. Методы и средства обеспечения ИБ. Современные принципы построения организационной культуры и ее значение для ИБ организации.

Тема 2. Понятие информационных угроз и их виды (ПК-1, ПК-2)
Информационные угрозы. Угрозы нарушения конфиденциальности информации. Информационная атака. Потенциальные злоумышленники (хакеры, крекеры). Информационные угрозы для государства, для компании (юридического лица), для личности (физического лица). Естественные и человеческие факторы информационных угроз (ИУ).
Нормы профессиональной этики. Нормы корпоративного управления и корпоративной культуры и ее роль в ИБ.
Классификация угроз безопасности информации. Несанкционированный доступ к защищаемой информации. Типовые пути несанкционированного доступа к информации

Тема 3. Государственное регулирование ИБ (ПК-1)

Ущерб от компьютерных злоупотреблений. Исторические аспекты борьбы органов уголовной юстиции с компьютерной преступностью (опыт США, стран Западной Европы, России). Меры, направленные на создание и поддержание в обществе негативного (в том числе карательного) отношения к нарушениям и нарушителям информационной безопасности.
Умение объяснять работникам проблемы управления рисками в организации и пути их решения в сфере ИБ. Международные договоры, доктрины в области ИБ. Информационные права граждан. Основные
законодательные по ИБ физических и юридических лиц в России (Конституция РФ, федеральные законы, Уголовный кодекс, Налоговый кодекс, Гражданский кодекс и др.).

Тема 4. Подходы, принципы, методы и средства обеспечения безопасности (ПК-1, ПК-2)
Управление защитой информации. Фрагментарный и комплексный подходы к защите информации. Характеристики методов средств ИБ экономического объекта. Криптография, механизмы цифровой подписи и особенности ее применения. Идентификация и аутентификация. Разграничения доступа. Протоколирование и аудит. Организационно-техническое обеспечение компьютерной безопасности. Организация конфиденциального делопроизводства. Программно-технические методы защиты информации. Виды служб безопасности, их место в аппарате управления предпринимательских структур различных типов. Менеджер по безопасности. Задачи службы безопасности, основные функции. Руководство и подчиненность. Типовая
структура службы безопасности.
Место, задачи, функции и структура подразделения (или
службы) конфиденциальной документации. Консультирования участников процесса управления рисками внутри организации.
Задачи и функции аналитического подразделения.
Задачи и функции подразделения охраны и пропускного режима. Задачи и функции подразделения инженерно-технической защиты информации. Задачи и функции других подразделений.
Взаимодействие службы безопасности и службы персонала. Организационные формы обеспечения безопасности в некрупных фирмах и малом бизнесе

Тема 5. Организация системы защиты информации (ПК-1, ПК-2)
Политика информационной безопасности. Принципы реализации политики безопасности. Этапы построения системы ИБ.

Тема 6. Менеджмент и аудит систем ИБ (ПК-2)
Оценка эффективности инвестиций в информационную безопасность. Основные принципы управления рисками информационной безопасности. Шестнадцать методов, используемые для реализации пяти принципов управления рисками. Оценка риска и определение потребности. Признание информационных ресурсов в качестве существенных (неотъемлемых) активов организации. Разработка практических процедур
оценки рисков, связывающих безопасность и требования бизнеса

7.2 Содержание практических занятий и лабораторных работ

Тема 2. Понятие информационных угроз и их виды (ПК-1, ПК-2)
Вредоносные программы. Разглашение и утечка конфиденциальной информации (КИ). Каналы утечки КИ. Исторические аспекты реализации информационных угроз. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации угроз ИБ. Способы воздействия угроз на информационные объекты. Проявления возможного ущерба. Идентификация угроз. Компьютерные
преступления и наказания. Исторические примеры и современность. Риски угроз информационным ресурсам.

Тема 3. Государственное регулирование ИБ (ПК-1)

Специальное законодательство в области информатизации информационных технологий и информационной безопасности – федеральные законы, их структура и содержание. Доктрина информационной безопасности России, принятая в 2016 году. Стандарты информационной безопасности. Правовые нормы ИБ в организациях. Законодательство в области интеллектуальной собственности, информационных ресурсов, информационных продуктов.
Повышение образовательной и правовой культуры населения в сфере ИБ.

Тема 4. Подходы, принципы, методы и средства обеспечения безопасности (ПК-1, ПК-2)
Профессиональные и психологические требования к сотрудникам службы безопасности. Плановая и контрольная работа в службе безопасности. Назначение и взаимосвязь плановой и контрольной работы службы безопасности. Их место в построении и функционировании комплексной системы защиты информации фирмы. Анализ и оценка надежности и эффективности применяемой системы защиты. Регламентированный и нерегламентированный контроль системы защиты. Цели и задачи планирования работы по формированию и совершенствованию системы защиты информации. Планирование работы службы. Стадии контроля; учет контрольных операций. Методы и средства защиты от вредоносных программ. Профилактика вирусного заражения программ. Защита информация в Интернете

Тема 5. Организация системы защиты информации (ПК-1, ПК-2)
Способы устранения (смягчения) воздействия непредвиденных ситуаций. Обеспечение ИБ автоматизированных банковских систем, электронной коммерции и др.

Тема 6. Менеджмент и аудит систем ИБ (ПК-2) Ответственность менеджеров бизнес-подразделений и менеджеров, участвующих в программе обеспечения безопасности. Непрерывное управление рисками. Централизованное управление. Определение бюджета и персонала. Профессионализм и технические знания сотрудников. Средства контроля. Контроль факторов, влияющих на риски и указывающих на эффективность информационной безопасности. Новые методы и средства контроля.

7.3. Содержание самостоятельной работы

Тема 2. Понятие информационных угроз и их виды (ПК-1, ПК-2) 1. Изучение основной и дополнительной литературы. 2. Решение практических и теоретических задач в соответствии с изучаемыми темами. 3. Подготовка к зачету (Приложение 2).
Тема 3. Государственное регулирование ИБ (ПК-1) 1. Изучение основной и дополнительной литературы. 2. Решение практических и теоретических задач в соответствии с изучаемыми темами. 3. Подготовка к зачету (Приложение 2).
Тема 4. Подходы, принципы, методы и средства обеспечения безопасности (ПК-1, ПК-2) 1. Изучение основной и дополнительной литературы. 2. Решение практических и теоретических задач в соответствии с изучаемыми темами. 3. Подготовка к зачету (Приложение 2).
Тема 5. Организация системы защиты информации (ПК-1, ПК-2) 1. Изучение основной и дополнительной литературы. 2. Решение практических и теоретических задач в соответствии с изучаемыми темами. 3. Подготовка к зачету (Приложение 2).
Тема 6. Менеджмент и аудит систем ИБ (ПК-2) 1. Изучение основной и дополнительной литературы. 2. Решение практических и теоретических задач в соответствии с изучаемыми темами. 3. Подготовка к зачету (Приложение 2).

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену
Приложение 1

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету/экзамену
Приложение 2

7.3.3. Перечень курсовых работ
Не предусмотрено

7.4. Электронное портфолио обучающегося
Материалы не размещаются в портфолио

7.5. Методические рекомендации по выполнению контрольной работы
Не предусмотрено

7.6 Методические рекомендации по выполнению курсовой работы
Не предусмотрено

8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

По заявлению студента

В целях доступности освоения программы для лиц с ограниченными возможностями здоровья при необходимости кафедра обеспечивает следующие условия:

- особый порядок освоения дисциплины, с учетом состояния их здоровья;
- электронные образовательные ресурсы по дисциплине в формах, адаптированных к ограничениям их здоровья;
- изучение дисциплины по индивидуальному учебному плану (вне зависимости от формы обучения);
- электронное обучение и дистанционные образовательные технологии, которые предусматривают возможности приема-передачи информации в доступных для них формах.
- доступ (удаленный доступ), к современным профессиональным базам данных и информационным справочным системам, состав которых определен РПД.

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Сайт библиотеки УрГЭУ
http://lib.usue.ru/

Основная литература:

2. Баранова Е.К., Бабаш А.В. Информационная безопасность. История специальных методов криптографической деятельности [Электронный ресурс]:учебное пособие. - Москва: Издательский Центр РИО, 2022. - 236 – Режим доступа: https://znanium.ru/catalog/product/1843171

3. Исаева О. М., Припорова Е. А. Управление человеческими ресурсами [Электронный ресурс]:Учебник и практикум для вузов. - Москва: Юрайт, 2022. - 178 – Режим доступа: https://urait.ru/bcode/490178

4. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации [Электронный ресурс]:учебное пособие. - Москва: Издательский Центр РИО, 2022. - 336 – Режим доступа: https://znanium.ru/catalog/product/1861657

5. Одинцов Б. Е. Когнитивные системы управления эффективностью бизнеса [Электронный ресурс]:учебник и практикум для вузов. - Москва: Юрайт, 2025. - 311 – Режим доступа: https://urait.ru/bcode/560630

6. Рыжко А. Л., Рыбников А. И., Рыжко Н. А. Информационные системы управления производственной компанией [Электронный ресурс]:учебник для вузов. - Москва: Юрайт, 2025. - 354 – Режим доступа: https://urait.ru/bcode/560486

7. Исаева О. М., Припорова Е. А. Управление человеческими ресурсами [Электронный ресурс]:учебник и практикум для вузов. - Москва: Юрайт, 2025. - 172 – Режим доступа: https://urait.ru/bcode/561222

Дополнительная литература:

2. Козьминых С.И. Информационная безопасность финансово-кредитных организаций в условиях цифровой трансформации экономики [Электронный ресурс]:Монография. - Москва: КноРус, 2021. - 281 – Режим доступа: https://book.ru/book/941548

3. Вершков А.В., Москалев А.К. Управление инновационной деятельностью [Электронный ресурс]:Учебное пособие. - Красноярск: Сибирский федеральный университет, 2020. - 168 – Режим доступа: https://znanium.com/catalog/product/1818934

4. Кузнецов И.Н. Бизнес-безопасность [Электронный ресурс]:Практическое пособие. - Москва: Издательско-торговая корпорация "Дашков и К", 2022. - 412 – Режим доступа: https://znanium.com/catalog/product/2082469

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Перечень лицензионного программного обеспечения:

Astra Linux Common Edition. Договор №0417-ПО/2019 от 08.05.2019, Акт №Sk000343 от 24.05.2019 и Контракт № 35-У/2018 от 13.06.2018, Акт № УТ213 от 17.12.2018. Срок действия лицензии - без ограничения срока.

Libre Office. Лицензия GNU LGPL. Срок действия лицензии - без ограничения срока.

МойОфис стандартный. Соглашение № СК-281 от 7 июня 2017. Дата заключения - 07.06.2017. Срок действия лицензии - без ограничения срока.

Перечень информационных справочных систем, ресурсов информационно-телекоммуникационной сети «Интернет»:

Справочно-правовая система Консультант +. Договор № 143/223-У/2025 от 02.12.2025 Срок действия лицензии до 31.12.2026

Справочно-правовая система Гарант. Договор № 58419 от 22 декабря 2015. Срок действия лицензии -без ограничения срока

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Реализация учебной дисциплины осуществляется с использованием материально-технической базы УрГЭУ, обеспечивающей проведение всех видов учебных занятий и научно-исследовательской и самостоятельной работы обучающихся:

Специальные помещения представляют собой учебные аудитории для проведения всех видов занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УрГЭУ.

Все помещения укомплектованы специализированной мебелью и оснащены мультимедийным оборудованием спецоборудованием (информационно-телекоммуникационным, иным компьютерным), доступом к информационно-поисковым, справочно-правовым системам, электронным библиотечным системам, базам данных действующего законодательства, иным информационным ресурсам служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа презентации и другие учебно-наглядные пособия, обеспечивающие тематические иллюстрации.

Приложение 1
к рабочей программе

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету с оценкой по дисциплине «Информационная политика организации»

1. Информационное общество. Информационное пространство. Информационная война и информационное противоборство.
2. Информационная преступность.
3. Угрозы безопасности информации.
4. Информационная безопасность (ИБ).
5. Политика безопасности. Объекты и субъекты обеспечения ИБ.
6. Методы и средства обеспечения ИБ.
7. Объекты ИБ на предприятии. Системный подход к защите информации.
8. Структура (подсистемы) системы ИБ.
9. Экономическая информация как товар и объект безопасности.
10. Информационные ресурсы и информационная безопасность.
11. Правовой режим информационных ресурсов. Информационно-правовые отношения.
12. Документирование информации как обязательное условие включения информации в информационные ресурсы.
13. Понятие ценной (собственной) предпринимательской информации.
14. Ценность и полезность информации.
15. Критерии ценности информационных ресурсов. Правовые и экономические предпосылки выделения ценной информации.
16. Информационные угрозы. Угрозы нарушения конфиденциальности информации. Информационная атака.
17. Потенциальные злоумышленники (хакеры, крекеры). Информационные угрозы для государства, для компании (юридического лица), для личности (физического лица).
18. Естественные и человеческие факторы информационных угроз (ИУ). Классификация угроз безопасности информации.
19. Несанкционированный доступ к защищаемой информации. Типовые пути несанкционированного доступа к информации
20. Ущерб от компьютерных злоупотреблений.
21. Исторические аспекты борьбы органов уголовной юстиции с компьютерной преступностью (опыт США, стран Западной Европы, России).
22. Меры, направленные на создание и поддержание в обществе негативного (в том числе карательного) отношения к нарушениям и нарушителям информационной безопасности.
23. Международные договоры, доктрины в области ИБ. Информационные права граждан. Основные законодательные по ИБ физических и юридических лиц в России (Конституция РФ, федеральные законы, Уголовный кодекс, Налоговый кодекс, Гражданский кодекс и др.).
24. Управление защитой информации. Фрагментарный и комплексный подходы к защите информации.
25. Характеристики методов средств ИБ экономического объекта. Криптография, механизмы цифровой подписи и особенности ее применения.
26. Идентификация и аутентификация. Разграничения доступа.
27. Протоколирование и аудит. Организационно-техническое обеспечение компьютерной безопасности.

28. Организация конфиденциального делопроизводства.
29. Программно- технические методы защиты информации.
30. Виды служб безопасности, их место в аппарате управления предпринимательских структур различных типов.
31. Менеджер по безопасности. Задачи службы безопасности, основные функции.
32. Руководство и подчиненность. Типовая структура службы безопасности.
33. Место, задачи, функции и структура подразделения (или службы) конфиденциальной документации. Задачи и функции аналитического подразделения.
34. Задачи и функции подразделения охраны и пропускного режима. Задачи и функции подразделения инженерно-технической защиты информации. Задачи и функции других подразделений.
35. Взаимодействие службы безопасности и службы персонала. Организационные формы обеспечения безопасности в некрупных фирмах и малом бизнесе.
36. Оценка эффективности инвестиций в информационную безопасность. Основные принципы управления рисками информационной безопасности.
37. Шестнадцать методов, используемые для реализации пяти принципов управления рисками.
38. Оценка риска и определение потребности.
39. Признание информационных ресурсов в качестве существенных (неотъемлемых) активов организации.
40. Разработка практических процедур оценки рисков, связывающих безопасность и требования бизнеса

Приложение 2
к рабочей программе

7.3.2. Практические задания для самостоятельной подготовки к зачету по дисциплине «Информационная политика организации»

Тема 1. Теоретические аспекты информационной безопасности экономических систем

Вопросы для обсуждения:

1. Взаимосвязь критериев ценности и необходимости обеспечения безопасности информации.
2. Понятие уязвимости информации.
3. Типовые классификационные группы ценной предпринимательской информации.
4. Информационные ресурсы государственные и негосударственные.
5. Классификация информационных продуктов и услуг.
6. Информационные ресурсы открытые и ресурсы ограниченного доступа и использования

ТЕСТ № 1.

ТЕСТ 1. на дескриптор «Знать: Информационная политика организации»

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
А. Разработка аппаратных средств обеспечения правовых данных
Б. Разработка и установка во всех компьютерных правовых сетях журналов учета действий
В. Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
А. Хищение жестких дисков, подключение к сети, инсайдерство
Б. Перехват данных, хищение данных, изменение архитектуры системы
В.Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:
А. Персональная, корпоративная, государственная
Б. Клиентская, серверная, сетевая
В. Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
А. несанкционированного доступа, воздействия в сети
Б. инсайдерства в организации
В. чрезвычайных ситуаций

5) Основные объекты информационной безопасности:
А. Компьютерные сети, базы данных
Б. Информационные системы, психологическое состояние пользователей
В. Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

А. Искажение, уменьшение объема, перекодировка информации
Б. Техническое вмешательство, выведение из строя оборудования сети
В. Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:
А. Экономической эффективности системы безопасности
Б. Многоплатформенной реализации системы
В. Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:
А. руководители, менеджеры, администраторы компаний
Б. органы права, государства, бизнеса
В. сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:
А. Установление регламента, аудит системы, выявление рисков
Б.Установка новых офисных приложений, смена хостинг-компании
В.Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:
А. Неоправданных ограничений при работе в сети (системе)
Б. Рисков безопасности сети, системы
В. Презумпции секретности

11) Принципом политики информационной безопасности является принцип:
А. Невозможности миновать защитные средства сети (системы)
Б. Усиления основного звена сети, системы
В. Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:
А. Усиления защищенности самого незащищенного звена сети (системы)
Б.Перехода в безопасное состояние работы сети, системы
В.Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:
В. Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
Б.Одноуровневой защиты сети, системы
В. Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:
А. Компьютерный сбой
Б. Логические закладки («мины»)
В. Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:
А. Прочитать приложение, если оно не содержит ничего ценного – удалить
Б. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
В. Удалить письмо с приложением, не раскрывая (не читая) его.

Задача №1

Вы – сотрудник лечебного учреждения. Ежедневно в базе данных происходит накопление большого количества информации.

1. Перечислите возможные способы способом обеспечения целостности и предотвращения уничтожения данных.

2. Определите, каким способом Вам необходимо воспользоваться. Объясните почему.

Задача №2

На доске объявлений размещено сообщение, в котором говорится о том, что каждому сотруднику организации выделяется персональный пароль. Для того чтобы сотрудники его не забыли, пароль представляет дату рождения и имя каждого сотрудника.

1. Какие правила обеспечения информационной безопасности нарушены?

2. Какие символы должны быть использованы при записи пароля?

Тема 2. Тема 2. Понятие информационных угроз и их виды

Вопросы для обсуждения

1. Вредоносные программы.
2. Разглашение и утечка конфиденциальной информации (КИ).
3. Каналы утечки КИ. Исторические аспекты реализации информационных угроз.
4. Личностно- профессиональные характеристики и действия сотрудников, способствующих реализации угроз ИБ.
5. Способы воздействия угроз на информационные объекты.
6. Проявления возможного ущерба. Идентификация угроз.
7. Компьютерные преступления и наказания.
8. Исторические примеры и современность. Риски угроз информационным ресурсам.

ТЕСТ № 2

1) Как называется принцип описывающий Секретность закрытого сообщения определяется секретностью ключа?_____

2) ЭЦП – это:_____

3) Назовите наиболее распространены угрозы информационной безопасности корпоративной системы:_____

4) Какое наиболее распространены угрозы информационной безопасности сети:_____

5) Назовите три наиболее распространенных средства воздействия на сеть офиса:_____,_____,_____

6) Утечкой информации в системе называется ситуация, характеризуемая:
_____

7) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
А. Целостность

Б. Доступность
В. Актуальность

8) Угроза информационной системе (компьютерной сети) – это:_____

9) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:_____

10) Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:_____

Задача №1

Вы – начальник информационной службы в ЛПУ. У вас возникли подозрения, что сотрудник вашей организации позволил себе неправомерный доступ к охраняемой законом компьютерной информации, что повлекло уничтожение и блокирование информации.

1. Какая статья уголовного кодекса была нарушена?

2. Какое наказание должен понести нарушитель?

Задача №2

Вы – руководитель отдела информационной безопасности организации. Вы подозреваете, что один из пользователей корпоративной информационной системы создает и распространяет вредоносные программы внутри сети.

1. Какая статья уголовного кодекса была нарушена?

2. Какое наказание должен понести нарушитель?

Тема 3. Государственное регулирование ИБ

Вопросы для обсуждения

1. Специальное законодательство в области информатизации информационных технологий и информационной безопасности – федеральные законы, их структура и содержание.
2. Доктрина информационной безопасности России, принятая в 2016 году.
3. Стандарты информационной безопасности.
4. Правовые нормы ИБ в организациях.
5. Законодательство в области интеллектуальной собственности, информационных ресурсов, информационных продуктов.
6. Повышение образовательной и правовой культуры населения в сфере ИБ.

Тест 3.

1. Каким нормативным актом регулируются отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации?

2. **Вставьте название пропущенных принципов:**
   Система обеспечения информационной безопасности информации должна базироваться на следующих четырех принципах:
   А._____
   Б._____
   В._____
   Г._____

3. Вставьте пропущенное выражение:

   К коммерческой тайне не могут быть отнесены:
   А._____
   Б. сведения о наличии свободных мест
   В. сведения о численности работников
   Г. сведения о противопожарной безопасности

4. Каким нормативным актом регулируются отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, на рынке товаров, работ, услуг и предупреждения недобросовестной конкуренции, а также определяет сведения, которые не могут составлять коммерческую тайну?

5. Вставьте пропущенное слово:
   _____ тайной может быть: защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной

   6) Какие степени секретности сведений, составляющих государственную тайну, существуют?

   7) Что такое информационная система персональных данных?

   8) Что такое государственная тайна?

   9) Основными составляющими информационной безопасности являются:

   10) Профессиональной тайной может быть:

Задача №1

Гражданин П. проник в информационную базу ККБ и скопировал интересующую его информацию с ограниченным доступом, о чем стало известно администраторам информационной системы. Через неделю ему пришла повестка в суд.

1. Являются ли его действия противозаконными?

2. С чем это связано?

3. Какое наказание может ждать гражданина П. за совершенные им действия?

Задача 2
Используя ГОСТ Р ИСО/МЭК 27002-2012, решить ситуационную задачу.
Вы – начальник отдела по вопросам информационной безопасности в некоторой некрупной организации (20-30 человек).
Вам необходимо разработать комплекс мероприятий (от 10 до 20) по следующему направлению: привлечение сторонних организаций к обработке информации.
Цель: обеспечение информационной безопасности при передаче ответственности за обработку информации другой организации.
Изучить разделы ГОСТ Р ИСО/МЭК 27002-2012.

Задача 3
Используя основные положения части 4, главы 70 Гражданского кодекса РФ, решить ситуационную задачу.
Гражданин Смирнов А.В. создал инструментальное программное средство для работы с трехмерной компьютерной графикой под названием «Albert 3D» и зарегистрировал на него свои права. 15.09.2019 этот гражданин заключил договор с компанией «MosTechnology» и передал свои имущественные права на распространение своего программного продукта сроком на один год. После заключения договора компания «MosTechnology» распространила версию программы «Albert 3D» с предварительной модификацией данного программного продукта без ведома автора.
Вопрос: Имеет ли место в данной ситуации нарушение авторского права гражданина Смирнова?
Ответ: согласно статьи №….

Тема 4. Подходы, принципы, методы и средства обеспечения безопасности

Вопросы для обсуждения

1. Профессиональные и психологические требования к сотрудникам службы безопасности.
2. Плановая и контрольная работа в службе безопасности.
3. Назначение и взаимосвязь плановой и контрольной работы службы безопасности
4. Их место в построении и функционировании комплексной системы защиты информации фирмы.
5. Анализ и оценка надежности и эффективности применяемой системы защиты.
6. Регламентированный и нерегламентированный контроль системы защиты.
7. Цели и задачи планирования работы по формированию и совершенствованию системы защиты информации.
8. Планирование работы службы.
9. Стадии контроля; учет контрольных операций.
10. Методы и средства защиты от вредоносных программ.
11. Профилактика вирусного заражения программ.
12. Защита информация в Интернете
13. Перечислите основополагающие документы по информационной безопасности.
14. Понятие государственной тайны.

15. Основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РФ.
16. Дайте характеристику Федерального закона от 27 июля 2006 г. № 149- ФЗ «Об информации, информационных технологиях и о защите информации».
17. Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных компьютерных программ?

ТЕСТ 4.

11) Что такое ИСПДн?

А. Информационная система персональных данных

Б. Личные данные сотрудников

В. Информация хранившаяся на сервере

Г. Система безопасности

12) Что такое целостность информации?

А. свойство информационных ресурсов, заключающееся в их неизменности в процессе передачи или хранения

Б. все меры, направленные на обеспечение информационной безопасности, должны планироваться с ранних стадий системы безопасности и вводиться своевременно

В. конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

Г. свойство информационных ресурсов, заключающееся в их получении и использовании по требованию уполномоченных лиц

13) Принцип системы обеспечения информационной безопасности «своевременности» предполагает, что:

А. свойство информационных ресурсов, заключающееся в их неизменности в процессе передачи или хранения

Б. все меры, направленные на обеспечение информационной безопасности, должны планироваться с ранних стадий системы безопасности и вводиться своевременно

В. конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

Г. свойство информационных ресурсов, заключающееся в их получении и использовании по требованию уполномоченных лиц

14) Что такое коммерческая тайна?

А. свойство информационных ресурсов, заключающееся в их неизменности в процессе передачи или хранения

Б. все меры, направленные на обеспечение информационной безопасности, должны планироваться с ранних стадий системы безопасности и вводиться своевременно

В. конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

Г. свойство информационных ресурсов, заключающееся в их получении и использовании по требованию уполномоченных лиц

15) Что такое доступность информации?
А. свойство информационных ресурсов, заключающееся в их неизменности в процессе передачи или хранения
Б. все меры, направленные на обеспечение информационной безопасности, должны планироваться с ранних стадий системы безопасности и вводиться своевременно
В. конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду
Г. свойство информационных ресурсов, заключающееся в их получении и использовании по требованию уполномоченных лиц

16) Какие типы ИС существуют?
А. Индивидуальные, военные
Б. Специальные, типовые
В. Секретные, типовые
С. Специальные, индивидуальные

17) Какой из нормативно-правовых документов определяет перечень объектов информационной безопасности и методы ее обеспечения?

18) К объектам служебной тайны относятся:
А. тайна страхования, тайна исповеди, врачебная тайна
Б. тайна следствия, военная тайна, судебная тайна
В. тайна связи, адвокатская тайна
Г. тайна личная, тайна хранения паролей, тайна паспортных данных

19) К объектам профессиональной тайне относятся:
А. тайна страхования, тайна исповеди, врачебная тайна, тайна связи, адвокатская тайна
Б. тайна следствия, военная тайна, судебная тайна
В. тайна личная, тайна хранения паролей, тайна паспортных данных

20) Что такое конфиденциальность информации?
А. свойство информационных ресурсов, заключающееся в их доступности для персонала
Б. свойство информационных ресурсов, заключающееся в их недоступности для неуполномоченных лиц
В. свойство информационных ресурсов, заключающееся в их недоступности для руководства
Г. свойство информационных ресурсов, заключающееся в их доступности для использования в деловой документации

Задача 1

Используя статьи УК РФ, ответьте на вопросы после ознакомления с ситуацией. Ситуация: А.Н. Иванов, сотрудник одного из филиалов ИТ-банка, внедрил в компьютерную банковскую систему вирус, уничтожающий исполняемые файлы (расширение .exe). В результате внедрения этого вируса было уничтожено 40 % банковских программных приложений, что принесло банку материальный ущерб в размере 780000 рублей. Вопросы: - Какая статья УК РФ была нарушена? - Что послужило предметом преступления? - Какие неправомерные информационные действия были совершены А.Н. Ивановым?

Задача 2
Вы – начальник отдела по вопросам информационной безопасности в некоторой некрупной организации (20-30 человек). Вам необходимо разработать требования к хранению, использованию и утилизации информации для вашей организации. Цель: обеспечение информационной безопасности при хранении, обработке, передаче и уничтожении информации.

Задача 3
Проработайте требования для специалистов по подбору кадров вашей организации с целью внесения пунктов об информационной безопасности в трудовой договор новых сотрудников. Цель: уведомление новых сотрудников о строгом выполнении требований по обеспечению информационной безопасности и ответственности за их нарушение.

Тема 5. Организация системы защиты информации

Вопросы для обсуждения

1. Способы устранения (смягчения) воздействия непредвиденных ситуаций.
2. Обеспечение ИБ автоматизированных банковских систем, электронной коммерции и др.

ТЕСТ 5

1. Продолжите фразу:
Мораль как один из способов регулирования поведения людей в обществе представляет собой ...

2. *Вставьте пропущенное слово:*
В соответствии со ст. 10 Всеобщей декларации прав человека каждый человек, для определения его прав и обязанностей и для установления обоснованности предъявленного ему уголовного обвинения, имеет право, на основе полного равенства, на то, чтобы его дело было рассмотрено гласно и с соблюдением всех требований _____ независимым и беспристрастным судом.

3. Выберите из предложенных вариантов правильный:

Профессиональная этика имеет значение, прежде всего для профессий, объектом которых является ...

А. право
Б. государство
В. человек
Г. культура

4. Выберите из предложенных вариантов правильный:

Учение о том. как должен поступать человек, какими принципами и нормами обязан руководствоваться. — это ...

А. прогностическая этика
Б. нравственная этика
В. эмпирическая этика
Г. прикладная этика

5. Вставьте пропущенное слово:
Совесть — это:
а) само-оценивающее чувство, переживание, один из древнейших интимно-личностных регуляторов поведения людей.
б) категория этики, характеризующая способность человека осуществлять нравственный самоконтроль, внутреннюю самооценку с позиций соответствия своего поведения требованиям нравственности, самостоятельно формулировать для себя нравственные задачи и требовать от себя их выполнения.

6. Вставьте пропущенное слово:

… – это совокупность моральных норм, которые определяют отношение человека к своему профессиональному долгу

7. **Выберите несколько вариантов ответов:**
Ответственность — это:
a) выражение ответственности человека за свое поведение перед самим собой, форма самоутверждения личности.
b) нравственную задачу, которую человек формулирует для себя сам на основании нравственных требований, обращенных ко всем.
c) категория этики, характеризующая личность с точки зрения выполнения ею нравственных требований, соответствия ее моральной деятельности нравственному долгу, рассматриваемого с позиций возможностей личности.
d) обязанность и необходимость давать отчет в своих действиях, поступках, отвечать за их возможные последствия.

8. Выберите несколько вариантов ответов:
Достоинство — это:
a) категория этики, означающая особое моральное отношение человека к самому себе и отношение к нему со стороны общества, окружающих, основанное на признании ценности человека как личности.
b) категория этики, характеризующая личность с точки зрения выполнения ею нравственных требований, соответствия ее моральной деятельности нравственному долгу, рассматриваемого с позиций возможностей личности.
c) мнение о нравственном облике человека, сложившееся у окружающих, основанное на его предшествующем поведении.
d) выражение ответственности человека за свое поведение перед самим собой, форма самоутверждения личности.

9. Выберите несколько вариантов ответов:
Репутация— это:
a) самооценивающее чувство, переживание, один из древнейших интимноличностных регуляторов поведения людей.
b) нравственная задача, которую человек формулирует для себя сам на основании нравственных требований, обращенных ко всем.
c) мнение о нравственном облике человека, сложившееся у окружающих, основанное на его предшествующем поведении.

d) выражение ответственности человека за свое поведение перед самим собой, форма самоутверждения личности.

10. Выберите один правильный вариант ответа:
Презумпция невиновности означает:
a) выражение ответственности человека за свое поведение перед самим собой, форма самоутверждения личности.
b) мнение о нравственном облике человека, сложившееся у окружающих, основанное на его предшествующем поведении.
d) признание достоинства и ценности личности.

11. Продолжите фразу:
Под профессиональной этикой понимается:

12.Вставьте пропущенные слова:
Под _____ _____ понимается система морально-нравственных принципов, стандартов и правил, которые приняты в определенной организации и регулируют поведение ее персонала. Это значит, что все работники компании обязаны демонстрировать по отношению к клиентам, партнерам и коллегам определенное отношение, соблюдать морально-этические принципы, которыми руководствуется данный бизнес.

13. **Выберите один правильный вариант ответа:**

Какая из функций корпоративной культуры заключается в достижении общего согласия на основе объединяющего действия важнейших элементов культуры, роста сплоченности коллектива:

а). ценностно-образующая;
б). коммуникационная;
в). мотивирующая;
г). познавательная;
д). стабилизационная;
ж). нормативно-регулирующая;
з). инновационная.

14. **Выберите один правильный вариант ответа:**

Какая из функций корпоративной культуры помогает организации выжить в условиях конкурентной борьбы:

а)ценностно-образующая;
б) коммуникационная;
в) мотивирующая;
г) познавательная;
д) стабилизационная;
ж) нормативно-регулирующая;
з) инновационная.

15. **Выберите один правильный вариант ответа:**

Какая из функций корпоративной культуры ведет к идентификации сотрудником себя с организацией:

а) ценностно-образующая;
б) коммуникационная;
в) мотивирующая;
г) познавательная;
ж) стабилизационная;
з) нормативно-регулирующая;
е) инновационная.

Практическая задача 1.

Дано пять информационных объектов:

- *компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия (отдел кадров);*
- *компьютер бухгалтера (бухгалтерия);*
- *личная банковская карта;*
- *школьный компьютер (компьютерный класс);*
- *компьютер – рабочая станция оператора (ТЭЦ).*

Для каждого из этих объектов указать не менее 7 угроз, которые могут быть реализованы по отношению к обрабатываемой в них информации, а также методы борьбы с данными угрозами.

Обозначить источник каждой из приведенных угроз.

Работу рекомендуется выполнять в таблице вида:

Таблица 1. Рекомендуемый вид таблицы

№ п/п	Наименование угрозы	Источник	Метод защиты от угрозы
Компьютер с конфиденциальной информацией о сотрудниках предприятия			
1.	…	…	…
Банковская карта			
1.	…	…	…
Компьютер бухгалтера			
1.	…	…	…
Компьютер в классе			
1.			
Рабочая станция оператора			
1.			

Практическая задача 2.

Составить характеристику вируса на основе варианта задания. Номером варианта задания является порядковый номер студента в списке группы

Таблица 2. Варианты задания

Номер варианта	Среда обитания	Способ заражения среды обитания	Способ воздействия	Особенности алгоритма
1	3	2	3	1
2	4	2	1	2
3	3	1	2	3
4	1	2	3	4
5	2	1	1	1
6	4	2	3	2
7	2	1	1	3
8	1	2	2	4
9	4	1	3	1
10	4	2	1	2
11	3	2	2	3
12	2	1	1	4
13	2	1	3	1
14	3	2	1	2
15	3	2	2	3
16	2	1	1	4
17	1	1	3	1
18	1	2	1	2
19	2	1	2	3
20	3	2	1	4
21	1	1	3	1
22	4	2	1	2
23	2	2	2	3
24	3	1	1	4
25	2	1	3	1
26	3	2	1	2
27	4	1	2	3
28	1	2	3	4
29	2	1	1	4
30	1	2	2	3

Практическая часть

1. Создайте файл virus.doc (содержание – чистый лист) и выполните алгоритм восстановления файла (в предположении его заражения макровирусом).
2. Зафиксируйте этапы работы, используйте команду PrintScreen клавиатуры (скопированные таким образом файлы вставьте в новый Wordдокумент для отчета).
3. Сравните размеры файлов virus.doc и virus.rtf, используйте пункты контекстного меню «Свойства» (для этого выделите в «Проводнике» файл, нажмите правую кнопку мыши и выберите пункт «Свойства»).

Контрольные вопросы

1. Что такое макровирус?
2. Какие типы файлов заражают макровирусы?
3. Как просмотреть код макровируса?
4. Как восстановить файл, зараженный макровирусом?

Тема 6. Менеджмент и аудит систем ИБ

Практическая часть 2.

1. Изучить теоретические основы шифрования шифрами простой замены (методом Цезаря и методом перестановки).

2. Зашифровать методом Цезаря предложение открытого текста для шифрования в соответствии с номером своего варианта.
3. Зашифровать (и расшифровать) методом перестановки одно слово открытого текста ключом, длина которого равна длине шифруемого слова. Слово задает преподаватель.
4. Придумать символьный пароль, преобразовать его в ключ и зашифровать (и расшифровать) фразу открытого текста с помощью этого ключа. Выберите предложение открытого текста для шифрования в соответствии с номером своего варианта (номером по списку группы):
   1. От добра добра не ищут.
   2. Кто рано встает, тот долго живет.
   3. Худой мир лучше доброй драки.
   4. Близок локоть, да не укусишь.
   5. Жизнь дана на добрые дела.
   6. Старый друг лучше новых двух.
   7. Сядем рядком да потолкуем ладком.
   8. Свято место пусто не бывает.
   9. Грамоте учиться всегда пригодится.
   10. Доброе слово и кошке приятно.
   11. Кто грамоте горазд, тому не пропасть.
   12. Дерево познается по его плодам.
   13. Из одной печи, да неодинаковы калачи.
   14. В чужой монастырь со своим уставом не ходят.
   15. Старый дуб не скоро сломится.
   16. Кашу маслом не испортишь.
   17. На чужой каравай рот не разевай.
   18. Доброму совету цены нет.
   19. Едешь на день, бери хлеба на неделю.
   20. В здоровом теле здоровый дух.
   21. Слышал звон, да не знает, где он.
   22. Не спеши языком, торопись делом.
   23. Всю жизнь живи, всю жизнь учись.
   24. Испокон века книга растит человека.
   25. Уменье работать дороже золота.
   26. Дважды молодым не бывать.
   27. Старый конь борозды не портит.
   28. Яблоко от яблони недалеко падает.
   29. Тише едешь, дальше будешь.
   30. На каждый роток не накинешь платок.

   Отчет должен содержать подробное описание шифрования и дешифрования с указанием исходного слова (текста), ключа шифрования, символьного и цифрового пароля, результата шифрования (шифротекста).

Контрольные вопросы

1. Что такое ключ?
2. Что такое криптосистема?
3. Пояснить, что такое шифрование и в чём заключается сущность метода Цезаря.
4. Пояснить, в чём заключается сущность метода перестановки.
5. Какие вы знаете основные алгоритмы шифрования?

ТЕМА 6. Менеджмент и аудит систем ИБ

Вопросы для обсуждения

1. Ответственность менеджеров бизнес-подразделений и менеджеров, участвующих в программе обеспечения безопасности.
2. Непрерывное управление рисками.
3. Централизованное управление.
4. Определение бюджета и персонала.
5. Профессионализм и технические знания сотрудников.
6. Средства контроля.
7. Контроль факторов, влияющих на риски и указывающих на эффективность информационной безопасности.
8. Новые методы и средства контроля.

ТЕСТ 6

1. Прогнозирование внешней экономической обстановки, стратегическое планирование, мониторинг социально-экономической и нормативно правовой среды, создание системы резервов – все это инструментарий:

А. методов диссипации риска

Б. методов компенсации риска

В. методов уклонения от риска

Г. методов локализации риска

2. ***Вставьте пропущенный метод:***

Основные методы управления рисками:

«_____ _____», «Лимитирование концентрации риска», «Хеджирование», «Диверсификация», «Распределение рисков», «Самострахование (внутреннее страхование)» .

3. ***Вставьте пропущенные слова:***

Под _____ _____ понимается: защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре

4. ***Вставьте пропущенное название:***

Для большинства компаний существует как минимум несколько внешних документов к управлению рисками, где перечислены требования или рекомендации в отношении управления рисками. Это могут быть новые изменения в законе об акционерных

обществах, ГОСТ Р ИСО31000, кодекс корпоративного управления ЦБ или методические рекомендации Росимущества, а также отраслевые стандарты и рекомендации, которые так или иначе затрагивают тему управления рисками. Первая задача внутреннего аудитора в рамках _____ _____ убедиться, что любые документы, упомянутые во внешних требованиях, разработаны и внедрены в организации.

5. Вставьте пропущенное слово:

COSO акцентирует внимание на пяти компонентах системы управления рисками организации:

1. *Руководство и _____*
2. *Стратегия и постановка целей*
3. *Производительность*
4. *Анализ и пересмотр*
5. *Информация, коммуникации и отчетность*

6. Выберите один правильный вариант ответа:

Защита информации:
а) небольшая программа для выполнения определенной задачи
б) комплекс мероприятий, направленных на обеспечение информационной безопасности +
в) процесс разработки структуры базы данных в соответствии с требованиями пользователей

7. Выберите один правильный вариант ответа:

Информационная безопасность зависит от:
а) компьютеров, поддерживающей инфраструктуры
б) пользователей
в) информации

8. Выберите один правильный вариант ответа:

Конфиденциальностью называется:
а) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
б) описание процедур
в) защита от несанкционированного доступа к информации

9. Выберите один правильный вариант ответа:

Для чего создаются информационные системы:
а) получения определенных информационных услуг
б) обработки информации
в) оба варианта верны

10. Выберите один правильный вариант ответа:

Кто является основным ответственным за определение уровня классификации информации:
а) руководитель среднего звена
б) владелец
в) высшее руководство

11. Выберите один правильный вариант ответа:

Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:
а) хакеры
б) контрагенты
в) сотрудники

12. Выберите один правильный вариант ответа:

Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству:
а) снизить уровень классификации этой информации
б) улучшить контроль за безопасностью этой информации
в) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

13. Выберите один правильный вариант ответа:

Что самое главное должно продумать руководство при классификации данных:
а) управление доступом, которое должно защищать данные
б) оценить уровень риска и отменить контрмеры
в) необходимый уровень доступности, целостности и конфиденциальности +

14. Выберите один правильный вариант ответа:

Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены:
а) владельцы данных
б) руководство
в) администраторы

15. Выберите один правильный вариант ответа:

Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании:
а) проведение тренингов по безопасности для всех сотрудников
б) поддержка высшего руководства
в) эффективные защитные меры и методы их внедрения

Лабораторная работа 1.

Цель: разработать политику безопасности объекта.

Задание: Гейм клуб «Pro.comP» хочет организовать областной турнир по Dota2. Однако состояние информационной безопасности в компании настораживает. Необходимо разработать
политику безопасности гейм клуба, ориентируясь в разработке на модель системы с полным перекрытием. Сформировать отчет по проделанной работе

Список оборудования: система для демонстрации отчета

Программное обеспечение: программа для демонстрации отчета

Теоретические сведения:

Политика безопасности организации – это важный документ, который разрабатывают в любой
информационной системе. В ней указывают уязвимости систем, возможные угрозы, нарушителей и
рекомендации по противостоянию им. Учитываются процедуры управления, сбора, обработки,
защиты и распределения информации. Регламентируется процедура разработки политики
безопасности специальными нормативно-правовыми документами, такими как, например, стандарт
ГОСТ Р ИСО/МЭК 15408-1-2013.

Порядок выполнения работы:

• Описать модель объекта (составляющие его компоненты, каналы обмена данными между ними
и внешними объектами, свойства информации, которые нуждаются в защите в каждой рассматриваемой ситуации);
• Описать модели угроз;
• Описать модели потенциальных нарушителей (как внешних, так и внутренних);
• Провести анализ рисков и отсеять наименее вероятные и менее фатальные по наносимому
ущербу угрозы;
• Сформировать рекомендации по внедрению средств защиты информации в клубе, рекомендации
по сотрудникам.

Содержанием отчета:

1. Цель работы.
2. Описание модели объекта.
3. Описание модели угроз.
4. Описание модели потенциальных нарушителей.
5. Анализ рисков.
6. Рекомендации по внедрению средств защиты информации.
7. Выводы.

Инструкция для учителя

Защиту данной лабораторной работы удобно организовать в виде соревнования. После рассказа ученика о своей политике безопасности, одноклассники могут предложить возможные
атаки, посоревноваться в пропущенных уязвимостях, предложить рекомендации по улучшению
политики безопасности.

Особое внимание рекомендуется уделить вопросу разумного выбора свойств, нуждающихся в защите (не забыть нужное, но и не писать все подряд, чтобы сэкономить ресурсы компании) и
доступных для защиты в конкретной ситуации (схемы ответственности за защиту свойств со стороны условного отправителя и условного получателя показывают, когда кто и что может защищать и в каких ситуациях это вообще невозможно)

	Алиса (клиент)	Боб
Ц	+	-
Д	-	-
К	+	+

Алиса (сервер)	Боб
+	-
+	-
+	+