Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Самарский государственный экономический университет»

Институт информационных систем

Кафедра информационных систем

УТВЕРЖДЕНО
Ученым советом Университета
(протокол № 9 от 31 мая 2022 г.)

РАБОЧАЯ ПРОГРАММА

Наименование дисциплины Б1.В.11 Информационная безопасность

Основная профессиональная образовательная программа 38.03.05 Бизнес-информатика программа ИТ-Предпринимательство

Квалификация (степень) выпускника бакалавр

Самара 2022

Содержание (рабочая программа)

Целью изучения дисциплины является формирование результатов обучения, обеспечивающих достижение планируемых результатов освоения образовательной программы.

1. Место дисциплины в структуре ОП

Дисциплина Информационная безопасность входит в часть, формируемая участниками образовательных отношений блока Б1.Дисциплины (модули)

Предшествующие дисциплины по связям компетенций: Решения SAP для бизнеса, Решения 1С для бизнеса, Управление ИТ-сервисами, Разработка и продвижение мобильных приложений, Корпоративные информационные системы, Анализ и моделирование бизнес-процессов, Базы данных, Проектирование информационных систем, Информационно-коммуникационные технологии в профессиональной деятельности, Технологии работы в социальных сетях

Последующие дисциплины по связям компетенций: Проектирование стартапа (базовый уровень), Управление интеллектуальным капиталом, Проектирование стартапа (продвинутый уровень)

2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

Изучение дисциплины Информационная безопасность в образовательной программе направлено на формирование у обучающихся следующих компетенций:

Профессиональные компетенции (ПК):

ПК-1 - Способен управлять операционной деятельностью организации в области ИТ

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ПК-1	ПК-1.1: Знать:	ПК-1.2: Уметь:	ПК-1.3: Владеть (иметь навыки):
	методы управления операционной деятельностью организации, ИТ – активами, проектами на основе международных и отечественных стандартов	организовывать процесс управления деятельностью организации, координировать процесс реализации ИТ - проекта, анализировать и моделировать поэтапное достижение целей ИТ – проекта	навыками управления операционной деятельностью организации, ИТ – проектами с учетом факторов внутренней и внешней среды

3. Объем и виды учебной работы

Учебным планом предусматриваются следующие виды учебной работы по дисциплине:

Очная форма обучения

Виды учебной работы	Всего час/ з.е.
	Сем 6
Контактная работа, в том числе:	54.15/1.5
Занятия лекционного типа	18/0.5
Занятия семинарского типа	36/1
Индивидуальная контактная работа (ИКР)	0.15/0
Самостоятельная работа:	35.85/1
Промежуточная аттестация	18/0.5
Вид промежуточной аттестации: Зачет	Зач
Общая трудоемкость (объем части образовательной	

программы): Часы	108
Зачетные единицы	3

4. Содержание дисциплины

4.1. Разделы, темы дисциплины и виды занятий:

Тематический план дисциплины Информационная безопасность представлен в таблице.

Разделы, темы дисциплины и виды занятий
Очная форма обучения

№ п/п	Наименование темы (раздела) дисциплины	Контактная работа				Самостоятельная работа	Планируемые результаты обучения в соотношении с результатами обучения по образовательной программе
		Лекции	Занятия семинарского типа: Практич. занятия	ИКР	ГКР		
1.	Законодательное и нормативное обеспечение информационной безопасности. Стандарты информационной безопасности	2				4	ПК-1.1, ПК-1.2, ПК -1.3
2.	Методологии оценки рисков и угроз информационной безопасности	4	16			8	ПК-1.1, ПК-1.2, ПК -1.3
3.	Аспекты информационной безопасности. Политика информационной безопасности	4				8	ПК-1.1, ПК-1.2, ПК -1.3
4.	Методы и средства защиты информации	4	20			8	ПК-1.1, ПК-1.2, ПК -1.3
5.	Реализация стратегии обеспечения безопасности информационных систем	4				7,85	ПК-1.1, ПК-1.2, ПК -1.3
	Контроль	18					
	Итого	**18**	**36**	**0.15**		**35.85**	

4.2 Содержание разделов и тем

4.2.1 Контактная работа

Тематика занятий лекционного типа

№п/п	Наименование темы (раздела) дисциплины	Вид занятия лекционного типа*	Тематика занятия лекционного типа
1.	Законодательное и нормативное обеспечение информационной безопасности. Стандарты информационной безопасности	лекция	Концептуальные документы национального уровня в области информационной безопасности
		лекция	Базовое законодательство в области информационных технологий и зашиты информации
		лекция	Руководящие документы и государственные стандарты России в области защиты информации и информационной безопасности
		лекция	Зарубежные стандарты и спецификации в системе менеджмента информационной

			безопасности
2.	Методологии оценки рисков и угроз информационной безопасности	лекция	Понятие и классификация угроз информационной безопасности
		лекция	Анализ угроз и источников их возникновения
		лекция	Понятие и классификация рисков
		лекция	Понятие и классификация атак
		лекция	Классификация компьютерных вирусов и вредоносных программ
3.	Аспекты информационной безопасности. Политика информационной безопасности	лекция	Основные принципы, направления и требования обеспечения информационной безопасности организации
		лекция	Концепция и политика информационной безопасности
		лекция	Методические основы построения системы информационной безопасности организации
		лекция	Формирование политики безопасности
4.	Методы и средства защиты информации	лекция	Понятие принципа комплексного использования методов и средств применительно к системе информационной безопасности
		лекция	Организационно-правовые способы охраны и защиты информации
		лекция	Криптографический и программно-технический аспекты информационной безопасности
5.	Реализация стратегии обеспечения безопасности информационных систем	лекция	Анализ информационной инфраструктуры организации
		лекция	Выбор приемлемой технологии управления рисками
		лекция	Разработка стратегии (плана) обеспечения информационной безопасности
		лекция	Реализация стратегии и оценка ее эффективности

*лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся

Тематика занятий семинарского типа

№п/п	Наименование темы (раздела) дисциплины	Вид занятия семинарского типа**	Тематика занятия семинарского типа
2.	Методологии оценки рисков и угроз информационной безопасности	практическое занятие	Использование механизмов защиты системного и прикладного ПО от атак на информационную систему
		практическое занятие	Построение системы информационной безопасности организации. Этап I.
		практическое занятие	Построение системы информационной безопасности организации. Этап II.
4.	Методы и средства защиты информации	практическое занятие	Программная реализация криптографических алгоритмов
		практическое занятие	Процедура аутентификации пользователя на основе пароля
		практическое занятие	Построение системы информационной безопасности организации. Этап III.

** семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные

занятия

Иная контактная работа

При проведении учебных занятий СГЭУ обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Формы и методы проведения иной контактной работы приведены в Методических указаниях по основной профессиональной образовательной программе.

4.2.2 Самостоятельная работа

№п/п	Наименование темы (раздела) дисциплины	Вид самостоятельной работы ***
1.	Законодательное и нормативное обеспечение информационной безопасности. Стандарты информационной безопасности	- тестирование
2.	Методологии оценки рисков и угроз информационной безопасности	- тестирование
3.	Аспекты информационной безопасности. Политика информационной безопасности	- тестирование
4.	Методы и средства защиты информации	- тестирование
5.	Реализация стратегии обеспечения безопасности информационных систем	- тестирование

*** самостоятельная работа в семестре, написание курсовых работ, докладов, выполнение контрольных работ

5. Материально-техническое и учебно-методическое обеспечение дисциплины

5.1 Литература:

Основная литература

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497002

Дополнительная литература

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490019

2. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2022. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489242

Литература для самостоятельного изучения

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2022. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1861657

5.2. Перечень лицензионного программного обеспечения

1. Microsoft Windows 10 Education / Microsoft Windows 7 / Windows Vista Business

2. Office 365 ProPlus, Microsoft Office 2019, Microsoft Office 2016 Professional Plus (Word, Excel, Access, PowerPoint, Outlook, OneNote, Publisher) / Microsoft Office 2007 (Word, Excel, Access,

PowerPoint)

3. GNU (свободно-распространяемое ПО): Open Office, Paint.net, Adobe Reader, Google Chrome, Yandex Browser, My Test, 1C Bitrix Demo, Spider Project Демо.

4. Project Expert 7 Tutorial 20

5. Лицензия (неисключительные права на использование программного обеспечения) на программный комплекс для расчетов и имитационного моделирования мультидисциплинарных систем MathWorks конфигурации Campus-Wide Suite

5.3 Современные профессиональные базы данных, к которым обеспечивается доступ обучающихся

1. Профессиональная база данных «Информационные системы Министерства экономического развития Российской Федерации в сети Интернет» (Портал «Официальная Россия» - http://www.gov.ru/)

2. Профессиональная база данных «Финансово-экономические показатели Российской Федерации» (Официальный сайт Министерства финансов РФ - https://www.minfin.ru/ru/)

3. Профессиональная база данных «Официальная статистика» (Официальный сайт Федеральной службы государственной статистики - http://www.gks.ru/)

5.4. Информационно-справочные системы, к которым обеспечивается доступ обучающихся

1. Справочно-правовая система «Консультант Плюс»

2. Справочно-правовая система «ГАРАНТ-Максимум»

5.5. Специальные помещения

Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мультимедийный проектор Доска Экран
Учебные аудитории для проведения практических занятий (занятий семинарского типа)	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС ГУУ и в электронно-библиотечную систему ГУУ
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС ГУУ и в электронно-библиотечную систему ГУУ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС ГУУ и в электронно-библиотечную систему ГУУ
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС ГУУ и в электронно-библиотечную систему ГУУ
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения оборудования

6. Фонд оценочных средств по дисциплине Информационная безопасность:

6.1. Контрольные мероприятия по дисциплине

Вид контроля	**Форма контроля**	**Отметить нужное знаком « + »**
Текущий контроль	Оценка докладов	-
	Устный/письменный опрос	+
	Тестирование	+
	Практические задачи	+
	Оценка проекта	-
Промежуточный контроль	Зачет	+

Порядок проведения мероприятий текущего и промежуточного контроля определяется Методическими указаниями по основной профессиональной образовательной программе высшего образования, утвержденными Ученым советом ФГАОУ ВО СГЭУ, протокол № 9 от 31.05.2022; Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном автономном образовательном учреждении высшего образования «Самарский государственный экономический университет»

6.2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

Профессиональные компетенции (ПК):

ПК-1 - Способен управлять операционной деятельностью организации в области ИТ

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	ПК-1.1: Знать:	ПК-1.2: Уметь:	ПК-1.3: Владеть (иметь навыки):
	методы управления операционной деятельностью организации, ИТ – активами, проектами на основе международных и отечественных стандартов	организовывать процесс управления деятельностью организации, координировать процесс реализации ИТ - проекта, анализировать и моделировать поэтапное достижение целей ИТ – проекта	навыками управления операционной деятельностью организации, ИТ – проектами с учетом факторов внутренней и внешней среды
Пороговый	основные методы управления операционной деятельностью организации, ИТ – активами, проектами	планировать процесс управления деятельностью организации, выполнять процесс реализации ИТ - проекта	Первоначальными навыками управления операционной деятельностью организации, ИТ – проектами
Стандартный (в дополнение к пороговому)	методы управления операционной деятельностью организации, ИТ – активами, проектами на основе международных	организовывать процесс управления деятельностью организации, координировать процесс реализации ИТ - проекта,	навыками управления операционной деятельностью организации, ИТ – проектами с учетом факторов внутренней и внешней среды

	и отечественных стандартов	анализировать и моделировать поэтапное достижение целей ИТ – проекта	
Повышенный (в дополнение к пороговому, стандартному)	прогрессивные методы управления операционной деятельностью организации, ИТ – активами, проектами на основе международных и отечественных стандартов	совершенствовать организацию процесса управления деятельностью организации, координировать и регулировать процесс реализации ИТ - проекта, анализировать и моделировать поэтапное достижение целей ИТ – проекта	навыками совершенствования управления операционной деятельностью организации, ИТ – проектами с учетом факторов внутренней и внешней среды в рамках решения целевых задач профессиональной проектной деятельности

6.3. Паспорт оценочных материалов

№ п/п	Наименование темы (раздела) дисциплины	Контролируемые планируемые результаты обучения в соотношении с результатами обучения по программе	Вид контроля/используемые оценочные средства	
			Текущий	Промежуточный
1.	Законодательное и нормативное обеспечение информационной безопасности. Стандарты информационной безопасности	ПК-1.1, ПК-1.2, ПК-1.3	Устный/письменный опрос Практические задачи Тестирование	Зачет
2.	Методологии оценки рисков и угроз информационной безопасности	ПК-1.1, ПК-1.2, ПК-1.3	Устный/письменный опрос Практические задачи Тестирование	Зачет
3.	Аспекты информационной безопасности. Политика информационной безопасности	ПК-1.1, ПК-1.2, ПК-1.3	Устный/письменный опрос Практические задачи Тестирование	Зачет
4.	Методы и средства защиты информации	ПК-1.1, ПК-1.2, ПК-1.3	Устный/письменный опрос Практические задачи Тестирование	Зачет
5.	Реализация стратегии обеспечения безопасности информационных систем	ПК-1.1, ПК-1.2, ПК-1.3	Устный/письменный опрос Практические задачи Тестирование	Зачет

6.4.Оценочные материалы для текущего контроля

Задания для выполнения точек академической активности и текущего контроля доступны по ссылке https://lms2.sseu.ru/course/index.php?categoryid=1910

Вопросы для устного/письменного опроса

Раздел дисциплины	Вопросы
Законодательное и нормативное обеспечение информационной безопасности. Стандарты информационной безопасности	1. Какие Вы знаете документы, регламентирующие информационную безопасность? 2. Какие законы регулируют область информационных технологий и защиты информации? 3. Перечислите документы и государственные стандарты России в области защиты информации и информационной безопасности 4. Перечислите зарубежные стандарты и спецификации в системе менеджмента информационной безопасности
Методологии оценки рисков и угроз информационной безопасности	5. Классификация угроз информационной безопасности 6. Назовите источники возникновения угроз информационной безопасности 7. Как формируется облик нарушителя? 8. Классифицировать угрозы автоматизированным системам 9. Классифицировать риски 10. Какие существуют методологии оценки рисков? 11. Как производится управление рисками? 12. Какие существуют компьютерные вирусы и вредоносные программы? 13. Перечислите методы противодействия атакам и последствиям от их реализации
Аспекты информационной безопасности. Политика информационной безопасности	14. Перечислить основные принципы обеспечения информационной безопасности организации 15. Перечислить основные направления обеспечения информационной безопасности организации 16. Перечислить основные требования обеспечения информационной безопасности организации 17. Что подразумевается под ценной информацией фирмы? 18. Как формируется политика безопасности?
Методы и средства защиты информации	19. В чем заключается принцип комплексного использования методов и средств применительно к системе информационной безопасности? 20. Перечислить организационно-правовые способы охраны и защиты информации 21. Какие технические средства защиты информации Вы знаете? 22. В чем заключается аутентификация и идентификация? 23. Перечислить методы защиты информации 24. Перечислить средства защиты информации 25. В чем заключается связь между способами и средствами защиты информации? 26. Какие административные процедуры защиты информации Вы знаете?
Реализация стратегии обеспечения безопасности информационных систем	27. В чем заключается анализ информационной инфраструктуры организации? 28. Как осуществляется выбор технологии управления рисками? 29. Проведите анализ остаточных рисков нарушения 30. Перечислите этапы стратегии обеспечения информационной безопасности 31. Какие существуют средства защиты? 32. Как осуществляется выбор средств защиты? 33. Как оценивается эффективность выбранной стратегии? 34. Какие действия необходимо предпринять для достижения стратегических целей развития безопасности информационных систем? 35. Какие задачи решаются на каждом этапе разработки стратегии обеспечения безопасности? 36. В чем заключаются риски реализации проекта разработки стратегии обеспечения безопасности?

	37. Для кого стратегия обеспечения безопасности информационных систем представляет интерес7

Задания для тестирования по дисциплине для оценки сформированности компетенций

1. Основными источниками угроз информационной безопасности являются все указанное в списке:

Перехват данных, хищение данных, изменение архитектуры системы
все ответы верны
Хищение жестких дисков, подключение к сети, инсайдерство
Хищение данных, подкуп системных администраторов, нарушение регламента работы

2. Виды информационной безопасности:

Персональная, корпоративная, государственная
Клиентская, серверная, сетевая
все ответы верны
Локальная, глобальная, смешанная

3. Цели информационной безопасности – своевременное обнаружение, предупреждение:

все ответы верны
чрезвычайных ситуаций
несанкционированного доступа, воздействия в сети
инсайдерства в организации

4. Основные объекты информационной безопасности:

Бизнес-ориентированные, коммерческие системы
все ответы верны
Компьютерные сети, базы данных
Информационные системы, психологическое состояние пользователей

5. Основными рисками информационной безопасности являются:

все ответы верны
Искажение, уменьшение объема, перекодировка информации
Потеря, искажение, утечка информации
Техническое вмешательство, выведение из строя оборудования сети

6. К основным функциям системы безопасности можно отнести все перечисленное:

все перечисленные
Установление регламента, аудит системы, выявление рисков
Установка новых офисных приложений, смена хостинг-компании
Внедрение аутентификации, проверки контактных данных пользователей

7. Наиболее распространены угрозы информационной безопасности сети:

Распределенный доступ клиент, отказ оборудования
Моральный износ сети, инсайдерство
Сбой (отказ) оборудования, нелегальное копирование данных

8. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

Актуальность
все ответы верны
Целостность
Доступность

9. Политика безопасности в системе (сети) – это комплекс:

Руководств, требований обеспечения необходимого уровня безопасности
Нормы информационного права, соблюдаемые в сети

Инструкций, алгоритмов поведения пользователя в сети

10. Криптографическое средство проставления ЭЦП – что это такое и где его можно приобрести?

11. Какие сертификаты можно использовать для подписи документов?

12. Если известны дата и номер документа, то эффективнее воспользоваться следующим видом поиска:
Быстрый поиск
Карточка поиска
Правовой навигатор

13. Компьютерная СПС - это программный комплекс ...
информационные технологии обработки информации
для хранения реквизитов правовых документов
массив правовой информации и программные инструменты

14. Процесс присвоения каждому документу определенного набора ключевых слов – это…
Администрирование
Инвентаризация
Инициализация
Индексация

15. Угроза информационной системе (компьютерной сети) – это:
Событие, происходящее периодически
Детерминированное (всегда определенное) событие
Вероятное событие

16. К основным принципам обеспечения информационной безопасности относится:
Усиление защищенности всех звеньев системы
все перечисленные
Экономическая эффективности системы безопасности
Многоплатформенная реализации системы

17. Основными субъектами информационной безопасности являются:
сетевые базы данных
все перечисленные
руководители, менеджеры, администраторы компаний
органы права, государства, бизнеса

18. Принципом информационной безопасности является принцип недопущения:
Рисков безопасности сети, системы
Презумпции секретности
все ответы верны
Неоправданных ограничений при работе в сети (системе)

19. Принципом политики информационной безопасности является принцип:
Невозможности миновать защитные средства сети (системы)
все перечисленные
Усиления основного звена сети, системы
Полного блокирования доступа при риск-ситуациях

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

все ответы верны

Практические задачи

Раздел дисциплины	Задачи
Методологии оценки рисков и угроз информационной безопасности	Разработать программу, имитирующую некоторые (см. вариант) действия по предупреждению вирусных угроз, обнаружению и удалению вирусных и других вредоносных программ и подготовить отчет о проделанной работе
	Изучить применение одного из алгоритмов симметричного шифрования; Осуществить шифрование с использованием алгоритма RSA. 1. Используя один из алгоритмов симметричного шифрования (см. вариант), зашифровать свои данные: фамилию, имя, отчество. 2. Выполнить проверку, расшифровав полученное сообщение. 3. Написать программу, реализующую алгоритм шифрования и дешифрования сообщения RSA. Входные данные: открытый и секретный ключи (значения n, e, d) и сообщение (m). 4. Используя заданные значения p, q, e, d (см. вариант) зашифровать и дешифровать сообщения m_1, m_2, m_3 (см. вариант).
Методы и средства защиты информации	Разработать программу, представляющую собой форму доступа к определённым информационным ресурсам на основе пароля: 1. В качестве информационного ресурса использовать любой файл или приложение. ***Для справки:*** работа с текстовым файлом в среде Delphi: `var myFile : TextFile;` `text : string;` `begin` `// Попытка открыть файл Test.txt для записи` `AssignFile(myFile, 'Test.txt');` `ReWrite(myFile);` `// Запись нескольких известных слов в этот файл` `WriteLn(myFile, 'Hello');` `WriteLn(myFile, 'World');` `// Закрытие файла` `CloseFile(myFile);` `// Открытие файла в режиме только для чтения` `FileMode := fmOpenRead;` `Reset(myFile);` `// Показ содержимого файла` `while not Eof(myFile) do` `begin` `ReadLn(myFile, text);` `ShowMessage(text);` `end;` `// Закрытие файла в последний раз` `CloseFile(myFile);` `end;` 2. Доступ к ресурсу должен быть разрешен только санкционированным пользователям. Для этого в программе должны храниться имена пользователей и их пароли. При попытке доступа пользователя к ресурсу проверяется наличие его идентификатора (имени) в системе и соответствие введенного пароля паролю, который хранится в системе. ***Для справки:*** Пример поиска элемента в массиве (Delphi): *// ввод массива for i:=l to SIZE do* *a[i] := StrToInt(StringGridl.Cells[i - 1, 0]);* *// ввод образца для поиска* *obr := StrToInt(edit2.text);* *// поиск* *found := FALSE; // пусть нужного элемента в массиве нет*

	i := 1; *repeat* *if a[i] = obr then* *found := TRUE* *else* *i := i + 1;* *until (i > SIZE) or (found = TRUE);* 3. В системе должна храниться следующая информация о пользователе: ID или имя пользователя, пароль, ФИО, дата рождения, место рождения (город) номер телефона. 4. Пользователь должен иметь возможность поменять пароль (ограничения: см. вариант).

6.5. Оценочные материалы для промежуточной аттестации

Фонд вопросов для проведения промежуточного контроля в форме зачета

Раздел дисциплины	Вопросы
Законодательное и нормативное обеспечение информационной безопасности. Стандарты информационной безопасности	1. Концептуальные документы национального уровня в области информационной безопасности 2. Базовое законодательство в области информационных технологий и зашиты информации. 3. Существующие законодательные нормы в составе ПНА, регулирующие вопросы информационной безопасности и защиты информации 4. Российские документы и государственные стандарты России в области защиты информации и информационной безопасности 5. Зарубежные стандарты и спецификации в системе менеджмента информационной безопасности
Методологии оценки рисков и угроз информационной безопасности	6. Понятие и классификация угроз информационной безопасности 7. Анализ угроз и источников их возникновения 8. Формирование облика нарушителя 9. Классификация угроз автоматизированным системам 10. Понятие уязвимости 11. Понятие и классификация рисков 12. Оценка рисков 13. Методология оценки рисков 14. Управление рисками 15. Понятие и классификация атак 16. Классификация компьютерных вирусов и вредоносных программ. 17. Методы противодействия атакам и последствиям от их реализации
Аспекты информационной безопасности. Политика информационной безопасности	18. Основные принципы, направления и требования обеспечения информационной безопасности организации 19. Концепция и политика информационной безопасности 20. Методические основы построения системы информационной безопасности организации 21. Определение состава и содержания ценной информации фирмы, подлежащей защите 22. Формирование политики безопасности
Методы и средства защиты информации	23. Понятие принципа комплексного использования методов и средств применительно к системе информационной безопасности 24. Организационно-правовые способы охраны и защиты информации 25. Административные процедуры 26. Криптографический и программно-технический аспекты информационной безопасности
Реализация стратегии обеспечения безопасности	27. Анализ информационной инфраструктуры организации 28. Выбор приемлемой технологии управления рисками 29. Анализ и оценка остаточных рисков нарушения

информационных систем	30. Разработка стратегии (плана) обеспечения информационной безопасности 31. Выбор средств защиты 32. Реализация стратегии и оценка ее эффективности

6.6. Шкалы и критерии оценивания по формам текущего контроля и промежуточной аттестации

Шкала и критерии оценивания

Оценка	**Критерии оценивания для мероприятий контроля с применением 2-х балльной системы**
«зачтено»	ПК-1
«не зачтено»	Результаты обучения не сформированы на пороговом уровне