ИНН 7715290332
ОГРН 1027739131375
127273, Москва, ул. Отрадная, д.6
тел.: +7(495) 736-92-70
e-mail: info@uni21.org
https://www.j-univer.ru

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки:
09.03.03 Прикладная информатика

Направленность (профиль)
Искусственный интеллект и анализ данных

Уровень высшего образования: бакалавриат

Москва – 2023

1. Цели и задачи дисциплины

Целью освоения дисциплины «Основы информационной безопасности» является: формирование у обучающихся базовых теоретических знаний в области информационной безопасности и развитие необходимых практических навыков их применения в будущей профессиональной деятельности.

Задачами освоения дисциплины «Основы информационной безопасности» являются:

- ознакомление с теорией и практикой обеспечения информационной безопасности;
- изучение основных требований и рекомендаций по защите информации, составляющей служебную информацию;
- овладение принципов формирования политики безопасности;
- формирование у обучаемого конкретных практических умений и навыков использования современных компьютерных средств и методов защиты данных.

2. Место дисциплины в структуре ОП бакалавриата

Дисциплина «Основы информационной безопасности» включена в перечень дисциплин учебного плана базовой части. Дисциплина «Основы информационной безопасности» реализуется в соответствии с требованиями ФГОС, ОПОП ВО и Учебного плана по направлению 09.03.03 Прикладная информатика, профиль «Прикладная информатика в экономике».

Предшествующими курсами, на которых непосредственно базируется дисциплина «Основы информационной безопасности», являются «Высшая математика», «Право в области IT», «Теоретические основы информатики», «Программирование».

Дисциплина «Основы информационной безопасности» считается основополагающей для изучения следующих дисциплин: «Интернет технологии в рекламе и связях с общественностью», «Интернет технологии в управлении производством», «Методы оптимальных решений», «Автоматизация учета на предприятии».

Особенностью дисциплины является то, что в процессе изучения дисциплины обучающиеся получают основные понятия в области информационной безопасности и методологические принципы создания систем защиты информации.

Рабочая программа дисциплины «Основы информационной безопасности» для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины «Основы информационной безопасности» позволит обучающемуся осуществлять трудовые действия в соответствии с профессиональным стандартом 06.015. «Специалист по информационным системам», утвержденным приказом Министерства труда и социальной защиты Российской Федерации от 18 ноября 2014г. № 896н:

- сбор исходных данных у заказчика;
- моделирование бизнес-процессов в ИС;
- анализ функциональных разрывов и корректировка на его основе существующей модели бизнес-процессов;
- согласование с заказчиком предлагаемых изменений;
- утверждение у заказчика предлагаемых изменений;
- документирование существующих бизнес-процессов организации заказчика (реверс-инжиниринг бизнес-процессов организации);
- адаптация бизнес-процессов заказчика к возможностям ИС

- выявление и анализ требований к ИС;
- создание (модификация) и сопровождение информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы в организациях различных форм собственности с целью повышения эффективности деятельности организаций-пользователей ИС
- оптимизация работы ИС;
- управление доступом к данным;
- сбор дополнительных материалов;
- подготовка итоговой отчетности.

В результате освоения дисциплины у обучающегося должны быть сформированы следующие компетенции:

Категория компетенций	Коды компетенции, ПС и ТФ (при наличии)	Формулировка компетенции	Индикаторы компетенции	Дескрипторы индикаторов
Общепрофессиональные компетенции	**ОПК-3**	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ОПК-3.1-** Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	**ОПК-3.1.1-** Демонстрируются поверхностные знания понятий информационной безопасности, характеристику ее составляющих; основные методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с учетом основных требований информационной безопасности. **ОПК-3.1.2-** Демонстрируются достаточные знания основных методов и средств решения стандартных задач

				профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. **ОПК-3.1.3-** Демонстрируются глубокие знания основных методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности и источники угроз информационной безопасности и меры по их предотвращению.
			ОПК-3.2- Умеет решать стандартные задачи профессиональной деятельности	**ОПК-3.2.1-** Демонстрируются знания современных средств и способов

			на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	обеспечения информационной безопасности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий. **ОПК-3.2.2-** Демонстрируется умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. **ОПК-3.1.3-** Демонстрируются отличные навыки и методологии создания систем защиты информации, применение основных правил и документов системы сертификации Российской Федерации, классификации основных угроз безопасности

				информации.
			ОПК-3.3- Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	**ОПК-3.3.1-** Минимальное владение навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности. **ОПК-3.3.2-** Достаточное владение навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности. **ОПК-3.3.3-** Уверенное и профессиональное владение основными понятиями в области информационной безопасности и методологическими принципами

				создания систем защиты информации, навыками подбора нормативных и методических материалов по вопросам обеспечения информационной безопасности.
Профессиональные компетенции	**ПК-3**	Способен разрабатывать, внедрять и адаптировать прикладное программное обеспечение с учетом требований информационной безопасности	**ПК-3.1-** Знает возможности типовой ИС, предметную область автоматизации, современные технологии разработки и адаптации прикладного программного обеспечения, их достоинства и недостатки; основы процесса внедрения информационных систем.	**ПК-3.1.1-** Демонстрируются поверхностные знания основных методов адаптации прикладного программного обеспечения, их достоинства и недостатки; основы процесса внедрения информационной безопасности. **ПК-3.1.2-** Демонстрируются достаточные знания основных современных технологий разработки и адаптации прикладного программного обеспечения, их достоинства и недостатки; основы процесса внедрения информационной безопасности. **ПК-3.1.3-** Демонстрируются глубокие знания основных возможностей оптимизации и исследования операций,

				математического и имитационного моделирования и построения эконометрических моделей объектов, явлений и процессов типовой ИС, предметную область автоматизации, современные технологии разработки и адаптации прикладного программного обеспечения, их достоинства и недостатки; основы процесса внедрения информационной безопасности.
			ПК-3.2- Умеет разрабатывать, адаптировать компоненты прикладного программного обеспечения; моделировать бизнес-процессы в ИС, работать в команде проекта по внедрению информационных систем.	**ПК-3.2.1-** Демонстрируются знания стандартных принципов работы в команде проекта по внедрению информационной безопасности. **ПК-3.2.2-** Демонстрируется умение адаптировать компоненты прикладного программного обеспечения; работать в команде проекта по внедрению информационных систем с учетом

				требований информационной безопасности. **ПК-3.2.3 -** Демонстрируются отличные навыки разработки, адаптации компоненты прикладного программного обеспечения; моделирования бизнес-процессов в ИС, работы в команде проекта по внедрению информационных систем с учетом требований информационной безопасности.
			ПК-3.3- Владеет навыками разработки прикладного программного обеспечения на современных языках программирования, методами адаптации прикладного программного обеспечения, бизнес-процессов заказчика к возможностям ИС.	**ПК-3.3.1-** Минимальное владение навыками разработки прикладного программного обеспечения на современных языках программирования, с учетом требований информационной безопасности. **ПК-3.3.2-** Достаточное владение навыками разработки прикладного программного обеспечения на современных языках программирования, методами

				адаптации прикладного программного обеспечения, бизнес-процессов заказчика к возможностям ИС с учетом требований информационной безопасности. **ПК-3.3.3-** Уверенное и профессиональное владение навыками разработки прикладного программного обеспечения на современных языках программирования, методами адаптации прикладного программного обеспечения, бизнес-процессов заказчика к возможностям ИС с учетом требований информационной безопасности.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

4.1. Структура дисциплины для очной формы обучения

Вид учебной работы	Всего часов	Трудоемкость по семестрам
		8 семестр
		144
Аудиторные занятия (всего)	32	32
Занятия лекционного типа	8	8
Занятия семинарского типа (практич., семин., лаборат. и др.)	24	24

Самостоятельная работа (всего)	76	76
Вид промежуточной аттестации (дифференцированный зачет, зачет, экзамен)	36	36
		Экзамен

4.2. Учебно-тематический план дисциплины

4.2.1. Учебно-тематический план дисциплины для очной формы обучения

Номер раздела	Наименование раздела/темы	Часов по учебной (рабочей) программе				
		Всего в уч. плане по разделу /теме	Аудиторная работа			Самостоятельная работа студента
			Всего	в том числе		
				Лекции (всего/интеракт.)	Практич занятия (всего/интеракт.)	
1	2	3	4	5	6	7
1	Тема 1. Основные понятия информационной безопасности. Нормативы и стандарты	36	10	2	8	25
2	Тема 2. Угрозы. Методы и средства защиты	36	10	2	8	25
3	Тема 3. Безопасность автоматизированных систем	36	12	4	8	26
	Контроль	36				36
	Итого	144	32	8	24	112

4.3. Содержание разделов и тем учебной дисциплины

Тема 1 Основные понятия информационной безопасности. Нормативы и стандарты

Понятие национальной и информационной безопасности РФ.

Государственная информационная политика. Государственная тайна.

Место информационной безопасности экономических систем в национальной безопасности страны.

Законодательная база информационной безопасности.

Доктрина информационной безопасности РФ.

Отечественные и зарубежные стандарты в области информационной безопасности.

Содержание практических занятий

- Освоение основных понятий и терминологии информационной безопасности;
- вирусные атаки и защита от них;
- изучение организационно-административных и технических методов и средств защиты информации;
- стандарты в области информационной безопасности;
- лабораторная работа «Шифрование данных».

Самостоятельная работа

- изучение материалов лекционных занятий, рекомендованной литературы и источников;
- подготовка к практическим занятиям;
- подготовка к лабораторной работе;
- подготовка домашних заданий и выполнение самостоятельной работы.

Тема 2 Угрозы. Методы и средства защиты

Понятие угрозы. Виды угроз. Нарушители информационной безопасности.

Характер происхождения угроз. Источники угроз. Предпосылки появления угроз.

Классификация угроз по способам их негативного воздействия.

Организационно-административные, технические, криптографические методы защиты информации.

Модели каналов передачи информации.

Коды, обнаруживающие и исправляющие ошибки.

Содержание практических занятий

- Знакомство с угрозами, которым подвергается информация, а также классификацией этих угроз;
- политика и уровни информационной безопасности;
- изучение криптографических методов защиты информации;
- идентификация и аутентификация, управление доступом;
- Система RSA;
- лабораторная работа «Сканируем сеть - Honeypot, Nmap».

Самостоятельная работа

- изучение материалов лекционных занятий, рекомендованной литературы и источников;
- подготовка к практическим занятиям;
- подготовка к лабораторной работе;
- подготовка домашних заданий и выполнение самостоятельной работы.

Тема 3 Безопасность автоматизированных систем

Информационные системы и связанные с их функционированием угрозы.

Возможные злоумышленные действия в автоматизированных системах обработки данных.

Модель нарушителя информационных систем. Модели оценки угроз. Модели защиты информации.

Цели, функции и задачи защиты информации в компьютерах и компьютерных сетях.

Архитектура механизмов защиты информации.

Разработка защищенных приложений в средах программирования.

Компьютерные вирусы и их классификация.

Принципы и средства защиты электронной почты и работы в интернет.

Методы защиты межсетевого обмена данными, использование межсетевых экранов.

Содержание практических занятий

- Изучение моделей информационной безопасности;
- методы определения требований к защите информации;
- классификация криптосистем, электронная подпись;
- обеспечение компьютерной и сетевой безопасности, особенности операционных систем Windows, Linux с точки зрения безопасности;
- способы заражения программ. Антивирусные программы;
- сетевая безопасность – хранение паролей, системы Active Directory, Kerberos;
- лабораторная работа «Межсетевой экран для ОС Windows».

Самостоятельная работа

- изучение материалов лекционных занятий, рекомендованной литературы и источников;
- подготовка к практическим занятиям;
- подготовка к лабораторной работе;
- подготовка домашних заданий и выполнение самостоятельной работы.

5. Индикаторы достижения компетенций и фонд оценочных средств для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

Преподавателю, для проверки сформированности у обучающихся компетенций по дисциплине, предоставляется право выбирать разноуровневые задания по своему усмотрению.

5.1. Индикаторы достижения компетенций на различных этапах их формирования

№ п/п	Компетенции	Оценка		
		Пороговый (удовлетворительно)	Продвинутый (хорошо)	Высокий (отлично)
1	**ОПК-3** Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности.			
Знать	Основные понятия информационной безопасности, принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Обучающийся демонстрирует плохое знание понятий информационной безопасности, характеристику ее составляющих; основные методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с учетом основных требований информационной безопасности.	Обучающийся демонстрирует знание основных методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Обучающийся демонстрирует отличное знание основных методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности и источники угроз информационной безопасности и меры по их предотвращению.
Уметь	самостоятельно решать стандартные	Плохо умеет решать задачи с применением	Умеет самостоятельно решать	Отлично умеет самостоятельно решать

	задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	современных средств и способов обеспечения информационной безопасности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий.	стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	стандартные профессиональные задачи с применением методологии создания систем защиты информации, применение основных правил и документов системы сертификации Российской Федерации, классификации основных угроз безопасности информации.
Владеть	навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Обучающийся демонстрирует плохое знание навыков подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Обучающийся демонстрирует знание методики подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Обучающийся демонстрирует отличное знание основных понятий в области информационной безопасности и методологических принципов создания систем защиты информации, навыков подбора нормативных и методических материалов по вопросам обеспечения информационной безопасности.
2	**ПК-3** Способен разрабатывать, внедрять и адаптировать прикладное программное обеспечение с учетом требований информационной безопасности.			
Знать	основные возможности типовой ИС, предметную область автоматизации, современные технологии разработки и	Обучающийся демонстрирует плохое знание основных методов адаптации прикладного программного обеспечения, их достоинства и	Обучающийся демонстрирует знание основных современных технологий разработки и адаптации прикладного программного	Обучающийся демонстрирует отличное знание основных возможностей типовой ИС, предметную область автоматизации,

	адаптации прикладного программного обеспечения, их достоинства и недостатки; основы процесса внедрения информационных систем с учетом информационной безопасности.	недостатки; основы процесса внедрения информационной безопасности.	обеспечения, их достоинства и недостатки; основы процесса внедрения информационной безопасности.	современные технологии разработки и адаптации прикладного программного обеспечения, их достоинства и недостатки; основы процесса внедрения информационных систем.
Уметь	самостоятельно решать разрабатывать, адаптировать компоненты прикладного программного обеспечения; моделировать бизнес-процессы в ИС, работать в команде проекта по внедрению информационных систем с учетом информационной безопасности.	Плохо умеет решать задачи с применением стандартных принципов работы в команде проекта по внедрению информационной безопасности.	Умеет самостоятельно адаптировать компоненты прикладного программного обеспечения; работать в команде проекта по внедрению информационных систем с учетом требований информационной безопасности.	Отлично умеет самостоятельно разрабатывать, адаптировать компоненты прикладного программного обеспечения; моделировать бизнес-процессы в ИС, работать в команде проекта по внедрению информационных систем с учетом требований информационной безопасности.
Владеть	навыками разработки прикладного программного обеспечения на современных языках программирования, методами адаптации прикладного программного обеспечения, бизнес-процессов заказчика к возможностям ИС с учетом	Обучающийся демонстрирует плохое знание навыков разработки прикладного программного обеспечения на современных языках программирования, с учетом требований информационной безопасности.	Обучающийся демонстрирует навыки разработки прикладного программного обеспечения на современных языках программирования, владение методами адаптации прикладного программного обеспечения, бизнес-процессов	Обучающийся демонстрирует отличное владение навыками разработки прикладного программного обеспечения на современных языках программирования, методами адаптации прикладного программного обеспечения, бизнес-процессов заказчика к

	требований информационной безопасности.		заказчика к возможностям ИС с учетом требований информационной безопасности.	возможностям ИС с учетом требований информационной безопасности.

5.2. Фонд оценочных средств дисциплины, отражающий этапы формирования компетенций

5.2.1. Типовые контрольные задания и материалы, необходимые для оценки знаний, умений, навыков, характеризующих этапы формирования индикаторов достижения компетенций по данной дисциплине

а) лабораторные работы по темам семестра:

1. Лабораторная работа №1 «Шифрование данных»

Цель: Получение теоретических и практических навыков работы с программными средствами шифрования данных TrueCrypt, PGP, GPG, LUCKS/dm-crypt.

Задания: Зашифровать и расшифровать файл(PGP). Создать криптоконтейнер TrueCrypt. Создать зашифрованную файловую систему.

1. Какие алгоритмы шифрования входят в комплект TrueCrypt?
2. Какие алгоритмы шифрования входят в комплект PGP, GPG?
3. Что такое «криптоконтейнер»?
4. Каковы основные достоинства и недостатки рассмотренных программных продуктов?
5. Какие алгоритмы шифрования, используемые в рассмотренных программных продуктах, наиболее надежны и почему?
6. В каких случаях рекомендуется применять шифрование данных?

2. Лабораторная работа №2 «Сканируем сеть - Honeypot, Nmap»

Цель: Получение практических и теоретических навыков работы с ловушкой honeypot, способами и методами сканирования сети.

Задания: Найти компьютеры в локальной сети (nmap). Создать ловушку honeypot. Убедится, что ловушка регистрирует попытки доступа к ней.

1. В чём заключается метод сканирование протоколов IP?
2. Перечислите основные методы сканирования Nmap.
3. На какие пакеты большинство ОС должны ответить флагом RST?
4. Назначение, цели, описание Honeypot.
5. Какие цели может преследовать злоумышленник, взламывая сервера?
6. Какое наказание предусмотрено в РФ за взлом?
7. Как выявлять Honeypot?
8. Что такое DHCP?
9. Для чего используется RPC-сканирование?

3. Лабораторная работа №3 «Межсетевой экран для ОС Windows»

Цель: ознакомиться с различными типами межсетевых экранов и теорией их построения на примере программы GNU SimpleWall и брандмауэра Windows.

Задания: настроить брандмауер на блокировку трафика программ и на отключение блокировки. Настроить межсетевой экран на блокировку исходящих соединений по порту 80. Убедиться, что сайты в интернете по HTTP не доступны. Блокировать ping. Убедиться, что пакеты уничтожаются экраном. Разблокировать доступ.

1. Как могут быть реализованы межсетевые экраны?
2. Перечислите достоинства межсетевого экрана прикладного уровня.
3. Перечислите недостатки межсетевого экрана с пакетной фильтрацией.
4. Выделите два основных типа межсетевых экранов.

5. Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией?

6. Можно ли использовать межсетевые экраны для защиты внутренних сетей от других внутренних систем?

7. Почему порядок правил в наборе правил межсетевого экрана играет важную роль?

б) письменное тестирование по темам семестра:

Задания для письменного тестирования:

Тест 1.

1. Информационная безопасность и ее основные компоненты.
2. Вирусные атаки и защита от них.
3. Сформировать открытый и секретный ключ в системе RSA (P=3, Q=5).
4. Зашифровать сообщение (4,8) с помощью криптосистемы Хилла (модуль равен 26, матрица $(■(1\&2@4\&5))$.

Тест 2.

1. Механизмы информационной безопасности.
2. Стандарты в области информационной безопасности.
3. Зашифровать сообщение x=3 в системе RSA (P=5, Q=7) с помощью ключа e=5.
4. Расшифровать сообщение (4,8) с помощью криптосистемы Хилла (модуль равен 26, матрица $(■(1\&2@4\&5))$.

Тест 3.

1. Политика информационной безопасности.
2. Уровни информационной безопасности.
3. Расшифровать сообщение x=4 в системе RSA (P=5, Q=7) с помощью ключа d=5.
4. Зашифровать сообщение «информация» с помощью шифра Цезаря.

Тест 4.

1. Принципы криптографической защиты информации.
2. Угрозы и способы обеспечения информационной безопасности.
3. Найти и объяснить, используемые в операционной системе Windows средства обеспечения конфиденциальности информации.
4. Закодировать с помощью метода Хаффмена слово «стандарт»

Тест 5.

1.Классификация криптосистем.

2.Электронная подпись, правовой и технический аспекты.

3. Найти и объяснить, используемые в операционной системе Windows средства обеспечения целостности информации.

4. Закодировать с помощью метода Фано слово «стандарт».

Тест 6.

1. Классификация компьютерных вирусов.
2. Способы распространения вирусов.
3. Троянские программы и их особенности.
4. Лечение компьютеных вирусов. Методы борьбы с ними.
5. Классификация антивирусных программ.

Тест 7.

1.Классификация компьютерных сетей с точки зрения безопасности.

2.Системы управления доступом. Сервера Kerberos и Active Directory.

3. Уязвимости компьютерных сетей. DDOS атаки. Эскалация привилегий. Ошибки в ПО. Человеческий фактор.

4. Основные способы взлома компьютерных сетей и защита от них.

в) тематика рефератов:

1. Виды защищаемой информации мероприятия по управлению доступом к информации.
2. Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.
3. Методы несанкционированного доступа к информации.
4. Основные способами привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.
5. Каналы утечки информации. Технические каналы утечки
6. Защита личности как носителя информации.
7. Системный подход к защите информации.
8. Этапы проектирования системы защиты информации.
9. Угрозы сохранности данных в компьютере случайного характера.
10. Классификация вирусов и антивирусных программ.
11. Компьютерная преступность. Виды преступной деятельности.
12. Криптографическая защита информации (основные понятия). Методы шифрования данных.
13. Проблемы региональной информационной безопасности.
14. Правовые, организационно-технические и экономические методы обеспечения информационной безопасности.
15. Компьютерная система как объект информационной безопасности.
16. Особенности обеспечения информационной безопасности в различных сферах общественной жизни.

г) перечень вопросов к экзамену

1. Информационная безопасность и ее основные компоненты.
2. Административный и процедурный уровни информационной безопасности.
3. Механизмы информационной безопасности.
4. Политика информационной безопасности.
5. Классификация атак, уровни безопасности.
6. Уязвимости и политика информационной безопасности.
7. Угрозы и способы обеспечения информационной безопасности
8. Стандарты в области информационной безопасности
9. Типы кодов, обнаруживающих и исправляющих ошибки, примеры.
10. Принципы криптографической защиты информации.
11. Симметричные и асимметричные криптосистемы.
12. Проблемы идентификации и проверки подлинности.
13. Электронная подпись, правовой и технический аспекты.
14. Межсетевые экраны и их предназначение.
15. Вирусные атаки и защита от них.
16. Классы моделей политик безопасности.
17. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации.
18. Понятие «информационная война».
19. Защита от деструктивного воздействия информации.
20. Информация ограниченного доступа.
21. Задачи информационной защиты в финансовой сфере.
22. Задачи информационной защиты в сфере предоставление услуг связи.
23. Организационно-распорядительные меры информационной защиты.
24. Специфика объектов информационной защиты.
25. Модель комплексной информационной защиты и ее элементы.
26. Модель информационной защиты каналов связи.
27. Формы и методы защиты признаковой информации.

5.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков

Критерии оценивания работы обучающихся на практических занятиях

Подача оценки преподавателя студентам должна соответствовать следующим критериям:

– предлагаемая оценка должна быть логически обоснованной, конкретной, чёткой, ясной и недвусмысленной;

– оценка должна производиться в позитивной атмосфере, способствующей развитию доверия и взаимопонимания между преподавателем и обучающимися;

– предметом оценки должна выступать текущая работа обучающегося в аудитории, его конкретные высказывания или действия, умения и навыки, способы взаимодействия с другими обучающимися;

– предметом оценки не могут выступать особенности внешности или личности обучающихся;

– критические замечания должны быть конструктивными и направленными на формирование, развитие и совершенствование у обучающихся недостающих или недостаточно полно сформированных компетенций;

– оценка должна быть понятной обучающемуся, предоставляться в соответствии с его индивидуально-психологическими особенностями и способами восприятия и переработки входящей информации. Для этого преподавателю важно выяснить, насколько правильно обучающийся понял данную ему оценку, насколько он с ней согласен или не согласен, как он к ней относится.

Критерии оценки результатов тестирования

– оценка «зачтено» – обучающийся правильно ответил на вопросы не менее чем 70% тестового задания (пример: если тестовое задание содержит 10 вопросов, для получения оценки «зачтено» обучающийся должен правильно ответить на 7 и более вопросов);

– оценка «не зачтено» – обучающийся правильно ответил на вопросы менее чем 70% тестового задания (пример: если тестовое задание содержит 10 вопросов, а обучающийся дал правильные ответы на 6 и менее вопросов, он получает оценку «не зачтено»).

Критерии оценки результатов выполнения лабораторных работ:

– оценка «отлично» – обучающийся сумел самостоятельно разобраться в задачах, предложенных в лабораторной работе. Оборудование и методы использованы правильно. Проявлена превосходная теоретическая подготовка. Необходимые навыки и умения полностью освоены. Результат лабораторной работы полностью соответствует её целям;

– оценка «хорошо» – обучающийся сумел разобраться в задачах, предложенных в лабораторной работе. Оборудование и методы использованы в основном правильно. Проявлена хорошая теоретическая подготовка. Необходимые навыки и умения в основном освоены. Результат лабораторной работы в основном

соответствует её целям;

– оценка «удовлетворительно» – обучающийся сумел разобраться в задачах, предложенных в лабораторной работе. Оборудование и методы частично использованы правильно. Проявлена удовлетворительная теоретическая подготовка. Необходимые навыки и умения частично освоены. Результат лабораторной работы частично соответствует её целям;

– оценка «неудовлетворительно» – не сумел самостоятельно разобраться в задачах лабораторной работы. Оборудование и методы использованы неправильно. Проявлена неудовлетворительная теоретическая подготовка. Необходимые навыки

и умения не освоены. Результат лабораторной работы не соответствует её целям.

Критерии оценивания реферата

– оценка «отлично» – работа сдана в указанные сроки, обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему, логично изложена собственная позиция, сформулированы выводы, раскрыта тема реферата, выдержан объем, соблюдены требования к внешнему оформлению;

– оценка «хорошо» – работа сдана в указанные сроки, обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему, слабо изложена собственная позиция, сформулированы выводы, раскрыта тема реферата, выдержан объем, соблюдены требования к внешнему оформлению;

– оценка «удовлетворительно» – основные требования к реферату выполнены, но при этом допущены недочеты, например: имеются неточности в изложении материала, отсутствует логическая последовательность в суждениях, объем реферата выдержан более чем на 50%, имеются упущения в оформлении;

– оценка «неудовлетворительно» – тема не раскрыта, обнаруживается существенное непонимание проблемы, допущены грубейшие ошибки в оформление работы, или реферат студентом не представлен.

Критерии оценки результатов устного экзамена

– оценка «отлично» – обучающийся демонстрирует глубокие знания материала учебной дисциплины и логично его излагает, свободно ориентируется в теоретических концепциях и их авторстве, владеет профессиональной терминологией, делает отсылки к профессиональной литературе и другим источникам, чётко видит и может продемонстрировать связь с другими разделами дисциплины, уверенно отвечает на вопросы, умеет увязать теоретические положения с практикой.

– оценка «хорошо» – обучающийся демонстрирует твердые знания материала учебной дисциплины и логично его излагает, знает основные теоретические концепции и их авторов, хорошо знаком с основной литературой, владеет профессиональной терминологией, способен отвечать на поставленные вопросы, не допуская при этом существенных неточностей, в целом умеет увязать теоретические знания с практическими решениями.

– оценка «удовлетворительно» – обучающийся демонстрирует базовые знания материала учебной дисциплины, допускает ошибки и неточности в его изложении, неуверенно ориентируется в профессиональной терминологии и источниковой базе, испытывает определённые трудности в увязке теоретического материала с практическими решениями.

– оценка «неудовлетворительно» – обучающийся демонстрирует слабое знание основ материала учебной дисциплины, допускает существенные ошибки и неточности в его изложении, плохо владеет профессиональной терминологией, не знаком с большинством теоретических концепций и их авторством, слабо ориентируется в источниковой базе дисциплины, не способен ответить на поставленные вопросы по существу, не умеет увязать теоретические знания с практическими решениями.

6. Учебно-методическое и информационное обеспечение дисциплины (включая самостоятельную работу)

а) основная литература

1. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 с.— Режим доступа: http://www.iprbookshop.ru/52209.html.

2. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная

Академия безопасности и выживания (МАБИВ), 2014.— 256 с.— Режим доступа: http://www.iprbookshop.ru/33430.html.

3. Авдошин С.М. Технологии и продукты Microsoft в обеспечении информационной безопасности [Электронный ресурс]/ Авдошин С.М., Савельева А.А., Сердюк В.А.— Электрон. текстовые данные.— Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017.— 412 с.— Режим доступа: http://www.iprbookshop.ru/72341.html.

б) дополнительная литература

1. Лапонина О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия [Электронный ресурс]/ Лапонина О.Р.— Электрон. текстовые данные.— Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 242 с.— Режим доступа: http://www.iprbookshop.ru/52217.html.

2. Фомин Д.В. Информационная безопасность [Электронный ресурс]: учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения/ Фомин Д.В.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 54 с.— Режим доступа: http://www.iprbookshop.ru/77320.html.

в) Интернет-ресурсы:

1. www.iprbookshop.ru – электорнно-библиотечная система.

7. Материально-техническое обеспечение дисциплины

Для выполнения практических, самостоятельных и контрольных работ подготовлены печатные материалы, которые содержатся в методической папке (кафедра информатики и математики), используются мультимедийные ресурсы кафедры и вуза.

Лекционные и практические занятия предполагают комплект презентационного оборудования: мультимедиа-проектор, ноутбук (или ПЭВМ).

Используемые программы (для подготовки и проведения занятий):

Microsoft Office 2019 Pro Plus (Word, Excel, PowerPoint, Access, Publisher, InfoPath); Adobe Reader; ESET NOD32 Antivirus; antiplagiat.ru, Научная электронная библиотека eLibrary.ru

Браузеры: Google Chrome, Mozilla Firefox, Opera

Медиапроигрыватели VLC Media Player, MPV

SaaS-платформа WIX, SaaS-платформа Tilda Publishing

Профессиональный интерфейс Яндекс.Директ, платформа Google Аналитика

Платформа разработки приложений для Android, iOs и Windows – Microsoft Visual Studio Community (включая библиотеку Monogame для Visual Studio)

Интегрированная среда для управления любой инфраструктурой SQL – Microsoft SQL Server Management Studio (SSMS)

Платформа для разработки Android-приложений Android Studio

Платформа Deductor Studio Academic

Microsoft Power BI Desktop

KNIME Analytics Platform

8. Особенности обучения лиц с ограниченными возможностями здоровья

Организация образовательного процесса для лиц с ограниченными возможностями здоровья осуществляется в соответствии с «Методическими рекомендациями по организации образовательного процесса для инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса» Министерства образования и науки Российской Федерации от 08.04.2014 г. № АК-44/05вн и «Положением об обучении

студентов-инвалидов и студентов с ограниченными возможностями здоровья», утвержденным ректором ОЧУ ВО «Еврейский университет» от 20.06.2019 г.

Подбор и разработка учебных материалов для обучающихся с ограниченными возможностями здоровья производится с учетом их индивидуальных особенностей.

Предусмотрена возможность обучения по индивидуальному графику.

Программа разработана Кучмезовым Х.Х.

Рабочая программа дисциплины рассмотрена и принята на заседании кафедры от 27.01.2022 г., протокол №6.

Лист регистрации изменений и дополнений в рабочую учебную программу

Составителем внесены следующие изменения:

Содержание изменений	**Номер протокола и дата заседания кафедры, по утверждению изменений**
Рабочая программа дисциплины дополнена и утверждена	№ 1 от 28.08.2023