ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа экономики и управления

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Карпушкина А. В.
Пользователь: karpushkinaav
Дата подписания: 15.02.2022

А. В. Карпушкина

РАБОЧАЯ ПРОГРАММА

дисциплины 1.Ф.П1.02 Основы безопасности IT-систем
для направления 38.03.05 Бизнес-информатика
уровень Бакалавриат
профиль подготовки Бизнес-информатика
форма обучения очная
кафедра-разработчик Цифровая экономика и информационные технологии

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 38.03.05 Бизнес-информатика, утверждённым приказом Минобрнауки от 29.07.2020 № 838

Зав.кафедрой разработчика,
д.экон.н., доц.

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Худякова Т. А.
Пользователь: khudiakovata
Дата подписания: 13.02.2022

Т. А. Худякова

Разработчик программы,
старший преподаватель

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Переведенцев В. В.
Пользователь: perevedentcevvv
Дата подписания: 13.02.2022

В. В. Переведенцев

СОГЛАСОВАНО

Руководитель образовательной программы
к.экон.н.

ЮУрГУ
Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Бородин С. И.
Пользователь: borodinsi
Дата подписания: 14.02.2022

С. И. Бородин

Челябинск

1. Цели и задачи дисциплины

Раскрыть сущность и понятие информационной безопасности; современную концепцию информационной безопасности; сущность и понятие «девиантного поведение в сфере информационно-коммуникативных технологий», его видов, диагностики и профилактики; познакомить с программно-техническими средствами обеспечения информационной безопасности, рассмотреть основные аспекты особенностей Интернет-общения, изучить нормы сетевого этикета, изучить методы анализа и оценки состояния обеспечения информационной безопасности в учреждении. Задачи дисциплины: - сформировать общее представление об информационной безопасности как о состоянии защищенности информационного ресурса сложной системы, понимание необходимости системного подхода к практической реализации такого состояния; - передать знания о порядке организации и практической реализации типовых мероприятий по обеспечению информационной безопасности и защите информации; - сформировать навыки анализа информационных ресурсов по следующим факторам: важность, конфиденциальность, уязвимость.

Краткое содержание дисциплины

Информационная безопасность — это процесс обеспечения конфиденциальности, целостности и доступности информации. Защищенность информационной среды организации — одно из основных условий ее эффективного функционирования. Комплекс мероприятий по обеспечению информационной безопасности информационной среды должен быть неотъемлемой частью системы управления любой организации. В настоящее время, персональные компьютеры (рабочие станции) пользователей, как правило, подключены к глобальной сети Интернет. Знания и умения пользователя по обеспечению информационной безопасности персонального компьютера, работающего в «агрессивной» сетевой среде, становятся одними из самых востребованных и необходимых. Данная дисциплина обеспечивает знакомство студента с теоретическими основами криптографии, инструментальными средствами и стандартами, поддерживающими разработку криптографического обеспечения информационных систем, практическими приемами защиты рабочих станций и серверов

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине
ПК-2 Способен выполнять работы по проектированию, созданию (модификации) и внедрению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы	Знает: последствия слабой защищенности информационных систем; принципы безопасного проектирования информационных систем на стадиях жизненного цикла; методы сбора данных для проектирования безопасных информационных систем; безопасные техники программирования Умеет: отстаивать позицию важности обеспечения информационной безопасности разрабатываемых информационных систем;

	определять потенциальные уязвимости и пути по их устранению; формировать входные данные для анализа защищенности информационных систем; находить потенциальные уязвимости в коде приложений Имеет практический опыт: оценки защищенности информационных систем на этапах проектирования; использования инструментов тестирования программ
ПК-4 Способен разрабатывать и управлять ИТ-сервисами предприятия и контентом Интернет-ресурсов	Знает: основные принципы административно-правовой защиты информации Умеет: быстро реагировать на различные угрозы информационной безопасности; применять современные технологии создания брандмауэров и IDS-комплексов Имеет практический опыт: применения, установки и настройки антивирусных систем и систем распознавания угроз и атак; обнаружения и защиты от атак
ПК-8 Способен готовить технико-экономическое обоснование проектов по совершенствованию и регламентации бизнес-процессов и ИТ-инфраструктуры предприятия	Знает: основы безопасности IT-систем Умеет: источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации классифицировать и оценивать угрозы информационной безопасности для объекта информатизации Имеет практический опыт: оценки защищенности программных прототипов решения прикладных задач; разработки документации для заказчика по совершенствованию ИС

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Архитектура корпоративных информационных систем, Web-программирование, CMS для разработки сайтов и Web приложений, Хранилища данных, Анализ данных и машинное обучение	CRM-системы, Производственная практика, преддипломная практика (8 семестр)

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
CMS для разработки сайтов и Web приложений	Знает: методы и средства, а также языки программирования для проектирования программного обеспечения, методы сбора и обработки информации, необходимой для

	решения поставленных задач; способы и методы расчета эффективности предлагаемых решений, форматы и способы хранения данных в интернете, стандарты и программные средства разработки web-приложений Умеет: разрабатывать web-ресурсы; тестировать web-приложение; выбирать и применять инструментальные средства для управления проектом, применять информационные технологии для решения поставленных задач; предлагать организационно-управленческие решения, приводящие к повышению экономической эффективности деятельности организации, определять связи между поставленными задачами и ожидаемые результаты их решения; в рамках поставленных задач определять имеющиеся ресурсы и ограничения, действующие правовые нормы Имеет практический опыт: программирования в среде Интернет; верификация программного кода относительно требований заказчика, сбора и анализа данных для решения поставленных задач; проведения маркетинговых исследований показателей деятельности организации, оценивания решение поставленных задач в зоне своей ответственности в соответствии с запланированными результатами контроля, при необходимости корректируя способы решения задач
Анализ данных и машинное обучение	Знает: методы предварительной обработки данных (переформатирования, устранения выбросов, заполнения пропусков, шкалирования, агрегации); методы классификации; методы кластеризации, основные принципы сбора информации, анализа полученных данных; методы сбора и анализа информации, инструменты и методы управления коммуникациями в проекте, технологии межличностной и групповой коммуникации в деловом взаимодействии Умеет: обоснованно выбирать наиболее подходящие алгоритмы решения задач машинного обучения и оценивать качество построенных моделей; строить с помощью методов машинного обучения формальные математические модели, интерпретировать их в терминах предметной области и формировать новые знания, применять машинное обучение в практической деятельности; проводить оценку эффективности полученных решений с точки зрения выбранных критериев, проводить анализ входной информации для решения практических задач; отслеживать и управлять рисками проекта Имеет практический опыт: построения и проверки качества формальных математических моделей; использования современных языков

	программирования для решения типичных задач машинного обучения: кластеризации, классификации, регрессии, описания возможных решений; обработки и анализа данных, разработки планов коммуникации с заказчиками
Хранилища данных	Знает: архитектуры и концепции хранилищ данных; технологии хранения (складирования) данных; теоретические основы многомерной модели данных; витрины данных; информационные потоки в хранилищах данных; классификацию программных продуктов для создания аналитических хранилищ данных; облачные хранилища и технологии, Проблемы интеграции информационных ресурсов в информационных хранилищах; основы современных систем управления базы данных, стандарты взаимодействия информационных систем; технологии хранения данных; модели данных, используемые для построения хранилищ; особенности построения систем на основе хранилищ данных; Умеет: выбирать систему хранения данных, соответствующую задачам профессиональной деятельности в соответствии с видом предпринимательской деятельности; проектировать многомерных базы данных, разрабатывать структуру базы данных; Создавать инфологические модели данных; выбирать системы хранения данных соответствующие сущности задач обработки информации, применять OLAP-технологию для анализа показателей электронной коммерции ; разрабатывать регламентирующие документы по хранению о обработки информации в базах данных; определять необходимость применения технологий интеллектуального анализа данных. Имеет практический опыт: настройки пользовательских инструментов промышленных хранилищ данных; разработки логических моделей хранилищ данных; интеграции информационных ресурсов в хранилищах данных, разработки структуры базы данных ИС; верификации структуры базы данных ИС относительно требований заказчика ИС, разработки логических моделей хранилищ данных
Архитектура корпоративных информационных систем	Знает: архитектура, устройство и функционирование вычислительных систем; инструменты и методы определения финансовых и производственных показателей деятельности организаций; основы общего управления организацией, методики описания и моделирования бизнес-процессов, средства моделирования бизнес-процессов; основные этапы проведения организационных изменений; основы реинжиниринга бизнес-процессов организации; , инструменты и методы анализа

	требований; устройство и функционирование современных ИС; современные подходы и стандарты автоматизации организации (например, CRM, MRP, ERP..., ITIL, ITSM); Умеет: осуществлять коммуникации; распределять работы и выделять ресурсы; тестировать результаты собственной работы, анализировать исходную документацию; анализировать функциональные разрывы; разрабатывать регламентную документацию, анализировать входные данные; проводить переговоры; подготавливать протоколы мероприятий; Имеет практический опыт: назначения и распределения ресурсов; обеспечения соответствия процессов модульного тестирования ИС принятым в организации или проекте стандартам и технологиям; настройки оборудования для оптимального функционирования ИС в соответствии с трудовым заданием;, верификации правильности установки ИС на рабочих местах заказчика; проектирования интерфейсов обмена данными в соответствии с трудовым заданием; информирования заказчика о возможностях типовой ИС и типовых технологиях ее создания (модификации) и ввода в эксплуатацию; , анализа функциональных и нефункциональных требований к ИС; информирования заказчика о возможностях типовой ИС и вариантах ее модификации; определения возможности достижения соответствия ИС первоначальным требованиям заказчика
Web-программирование	Знает: теорию процессного управления, принципы классификации процессов, методы структурирования процессов, основы операционного менеджмента, методы сбора информации., методики разработки контента и ИТ - сервисов предприятия и Интернет-ресурсов методы и способы управления контентом предприятия и Интернет-ресурсов, процессами создания и использования информационных сервисов (контент- сервисов), основы межкультурной коммуникации Умеет: применять принципы процессного управления, инструменты и методы операционного менеджмента, анализа, использовать современные языки программирования для разработки ИТ- сервисов предприятия; управлять контентом предприятия, процессами создания и предприятия, использования информационных сервисов (контент- сервисов), вести коммуникацию с представителями иных национальностей и конфессий с соблюдением этических и межкультурных норм Имеет практический опыт: владения методами сбора информации о процессе подразделения,

	навыками оценки эффективности деятельности подразделения , разработки контента и ИТ-сервисов предприятия и Интернет-ресурсов; работы с контентом предприятия, процессами создания и использования информационных сервисов (контент- сервисов), Анализа философских и исторических фактов, опыт оценки явлений культуры

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 2 з.е., 72 ч., 36,25 ч. контактной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		7
Общая трудоёмкость дисциплины	72	72
Аудиторные занятия:	32	32
Лекции (Л)	16	16
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	16	16
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	35,75	35,75
с применением дистанционных образовательных технологий	0	
Работа по разработке электронных приложений	15	15
Подготовка к зачету	10,75	10.75
Работа в письменной форме с устным докладом	10	10
Консультации и промежуточная аттестация	4,25	4,25
Вид контроля (зачет, диф.зачет, экзамен)	-	зачет

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Информационная безопасность и уровни ее обеспечения	6	2	4	0
2	Компьютерные вирусы и защита от них	8	4	4	0
3	Информационная безопасность вычислительных сетей	8	4	4	0
4	Механизмы обеспечения "информационной безопасности"	8	6	2	0
5	Понятие социального хакинга, "безопасное" поведение в информационной среде	2	0	2	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во

			часов
1	1	Понятие "информационная безопасность". Система формирования режима информационной безопасности. Стандарты информационной безопасности: "Общие критерии". Стандарты информационной безопасности распределенных систем	2
2	2	Классификация компьютерных вирусов	2
3	2	Антивирусные программы. Профилактика компьютерных вирусов	2
4	3	Особенности обеспечения информационной безопасности в компьютерных сетях. Адресация в глобальных сетях	2
5	3	Классификация удаленных угроз в вычислительных сетях. Методы разграничение доступа; Технология виртуальных частных сетей (VPN).	2
6	4	Криптография и шифрование	2
7-8	4	Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Криптографическая система RSA. Криптосистемы. Простые криптосистемы.	4

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Понятие "информационная безопасность"; Составляющие информационной безопасности. Задачи информационной безопасности общества; Уровни формирования режима информационной безопасности .	2
2	1	Требования безопасности к информационным системам; Сервисы безопасности в вычислительных сетях. Стандарты информационной безопасности в РФ; Административный уровень обеспечения информационной безопасности; Классификация угроз "информационной безопасности".	2
3	2	Компьютерные вирусы и информационная безопасность; Классификация компьютерных вирусов. Особенности работы антивирусных программ; Классификация антивирусных программ; Правила защиты от компьютерных вирусов	2
4	2	Виды "вирусоподобных" программ; Утилиты скрытого администрирования. Обнаружение загрузочного вируса; Обнаружение загрузочного вируса.	2
5	3	Особенности информационной безопасности в компьютерных сетях; Принципы организации обмена данными в вычислительных сетях.	2
6	3	Адресация в глобальных сетях.	2
7	4	Классификация систем шифрования данных; Механизм электронной цифровой подписи.	2
8	5	Мандатное и дискретное управление доступом; Определение и содержание регистрации и аудита информационных систем. Межсетевое экранирование; Технология виртуальных частных сетей (VPN).	2

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС			
Подвид СРС	Список литературы (с указанием разделов, глав, страниц) / ссылка на ресурс	Семестр	Кол-во часов
Работа по разработке электронных приложений	Климентьев, К.Е. Компьютерные вирусы и антивирусы: взгляд программиста. [Электронный ресурс] — Электрон. дан. — М. : ДМК Пресс, 2013. — 656 с.; Курило, А.П. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1. [Электронный ресурс] / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 244 с.; Шаньгин, В.Ф. Информационная безопасность. [Электронный ресурс] — Электрон. дан. — М. : ДМК Пресс, 2014. — 702 с.	7	15
Подготовка к зачету	Климентьев, К.Е. Компьютерные вирусы и антивирусы: взгляд программиста. [Электронный ресурс] — Электрон. дан. — М. : ДМК Пресс, 2013. — 656 с.; Курило, А.П. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1. [Электронный ресурс] / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 244 с.; Шаньгин, В.Ф. Информационная безопасность. [Электронный ресурс] — Электрон. дан. — М. : ДМК Пресс, 2014. — 702 с.	7	10,75
Работа в письменной форме с устным докладом	Климентьев, К.Е. Компьютерные вирусы и антивирусы: взгляд программиста. [Электронный ресурс] — Электрон. дан. — М. : ДМК Пресс, 2013. — 656 с.; Курило, А.П. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1. [Электронный ресурс] / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 244 с.; Шаньгин, В.Ф. Информационная безопасность. [Электронный ресурс] — Электрон. дан. — М. : ДМК Пресс, 2014. — 702 с.	7	10

6. Текущий контроль успеваемости, промежуточная аттестация

Контроль качества освоения образовательной программы осуществляется в соответствии с Положением о балльно-рейтинговой системе оценивания результатов учебной деятельности обучающихся.

6.1. Контрольные мероприятия (КМ)

№ КМ	Се-местр	Вид контроля	Название контрольного мероприятия	Вес	Макс. балл	Порядок начисления баллов	Учи-тыва-ется в ПА
1	7	Текущий контроль	Защита доклада	1	6	Для подготовки к докладу студентам выдаются темы для самостоятельного изучения. Доклад по теме готовится индивидуально. Защита доклада сопровождается презентацией, ответами на вопросы. При оценивании результатов мероприятия используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179) Показатели оценивания: - содержание: 2 балла – содержание полностью соответствует теме доклада, тема раскрыта полностью; 1 балл – содержание доклада не полностью соответствует теме и/или раскрыты не все аспекты темы; 0 баллов – содержание доклада не соответствует теме. - - оформление: 2 балла – презентация оформлена в соответствии с выданным заданием; 1 балл – в презентации выявлены недочеты; 0 баллов – студент неверно оформил презентацию или не выполнил задание. - срочность: 2 балла – доклад защищен в назначенный срок; 1 балл – доклад защищен на следующем занятии или консультации, после назначенного срока; 0 баллов – доклад защищен позднее, чем на следующем занятии или консультации.	зачет
2	7	Текущий контроль	Установка виртуальной машины для стенда	1	5	Группа делится на мини группы по 2 человека. Каждой подгруппе выдается индивидуальное задание, связанное с созданием виртуальной машины. При оценивании результатов работы используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). 5 баллов выставляется если студент демонстрирует правильно созданную сеть виртуальных машин, проведено правильное конфигурирование виртуальных машин, правильно и четко	зачет

						отвечает на вопросы по работе, понимает и разбирается в терминах; 4 балла выставляется если студент демонстрирует конфигурацию виртуальных машин с ошибками, но при защите с помощью преподавателя исправляет их, понимает и разбирается в терминах, отвечает на вопросы преподавателя с уточнением; 3 балла выставляется если студент демонстрирует созданные виртуальные машины с ошибками, правильно и четко отвечает на вопросы, понимает и разбирается в терминах; 2 балла выставляется если студент демонстрирует созданныую сеть виртуальных машин с ошибками и при защите не все ошибки может исправить, на вопросы отвечает с уточнением; 1 балл выставляется если студент создал сеть виртуальных машин с грубыми ошибками, на вопросы преподавателя отвечает с замечаниями; 0 баллов выставляется если студент не демонстрирует виртуальную машину или не может ответить на вопросы преподавателя.	
3	7	Текущий контроль	Тестирование	1	20	Тест состоит из 20 вопросов, позволяющих оценить сформированность компетенций. На ответы отводится 10 минут. Правильный ответ на вопрос соответствует 1 баллу. Неправильный ответ на вопрос соответствует 0 баллов	зачет
4	7	Проме-жуточная аттестация	Зачет	-	15	Зачет проводится в устной форме. Каждому студенту выдается билет с 3 вопросами. Время на подготовку отводится 30 минут. За каждый вопрос выставляется баллы. Максимальный балл за вопрос - 5. 5 баллов - Грамотный полный (развернутый) ответ на теоретический вопрос; 4 балла - дан правильный, но краткий ответ на вопрос; 3 балла - дан в общем правильный ответ на вопрос, но с замечаниями; 2 балла - дан неполный ответ на вопрос, но на уточняющие вопросы отвечено; 1 балл - дан неправильный ответ на вопрос, но на уточняющие вопросы даны правильные ответы; 0 -баллов - ответ на вопрос не дан.	зачет

6.2. Процедура проведения, критерии оценивания

Вид промежуточной аттестации	Процедура проведения	Критерии оценивания
зачет	Зачет проводится устно по билетам. Каждый билет содержит 3 вопроса, позволяющих оценить сформированность	В соответствии с пп. 2.5, 2.6

	компетенций. На подготовку дается 30 минут, после чего студент отвечает на вопросы в билете. Для уточнения уровня знаний студента преподаватель может задать от одного до трех дополнительных вопросов по темам курса. Результирующая оценка выставляется на основе полученных оценок за контрольно-рейтинговые мероприятия текущего контроля и промежуточной аттестации. При оценивании результатов учебной деятельности обучающегося по практике используется балльно-рейтинговая система оценивания результатов учебной деятельности обучающихся (утверждена приказом ректора от 24.05.2019 г. № 179). Зачтено выставляется если величина рейтинга учащегося 60-100%; не зачтено выставляется если величина рейтинга учащегося составляет менее 60%.	Положения

6.3. Оценочные материалы

Компетенции	Результаты обучения	№ КМ			
		1	2	3	4
ПК-2	Знает: последствия слабой защищенности информационных систем; принципы безопасного проектирования информационных систем на стадиях жизненного цикла; методы сбора данных для проектирования безопасных информационных систем; безопасные техники программирования	+	+	+	+
ПК-2	Умеет: отстаивать позицию важности обеспечения информационной безопасности разрабатываемых информационных систем; определять потенциальные уязвимости и пути по их устранению; формировать входные данные для анализа защищенности информационных систем; находить потенциальные уязвимости в коде приложений	+	+	+	+
ПК-2	Имеет практический опыт: оценки защищенности информационных систем на этапах проектирования; использования инструментов тестирования программ		+		+
ПК-4	Знает: основные принципы административно-правовой защиты информации	+	+	+	+
ПК-4	Умеет: быстро реагировать на различные угрозы информационной безопасности; применять современные технологии создания брандмауэров и IDS-комплексов	+	+	+	+
ПК-4	Имеет практический опыт: применения, установки и настройки антивирусных систем и систем распознавания угроз и атак; обнаружения и защиты от атак		+		+
ПК-8	Знает: основы безопасности IT-систем	+	+	+	+
ПК-8	Умеет: источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации классифицировать и оценивать угрозы информационной безопасности для объекта информатизации	+	+	+	+
ПК-8	Имеет практический опыт: оценки защищенности программных прототипов решения прикладных задач; разработки документации для заказчика по совершенствованию ИС		+		+

Фонды оценочных средств по каждому контрольному мероприятию находятся в приложениях.

7. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

1. Олифер, В. Г. Компьютерные сети : принципы, технологии, протоколы [Текст] учеб. для вузов по направлению 552800 "Информатика и вычисл. техника" и по специальностям 220100 "Вычисл. машины, комплексы, системы и сети", 220200 "Автоматизир. системы обработки информ. и упр.", 220400 "Програм. обеспечение вычисл. техники и автоматизир. систем" В. Г. Олифер, Н. А. Олифер. - 3-е изд. - СПб. и др.: Питер, 2008. - 957 с. ил.

б) дополнительная литература:

1. Компьютерные технологии в имитационном моделировании экономических процессов на предприятии и в научных исследованиях [Текст] учеб. пособие по направлению 080100 "Экономика" и др. направлениям Л. А. Баев и др.; Юж.-Урал. гос. ун-т, Каф. Экономика и упр. проектами ; ЮУрГУ. - Челябинск: Издательский Центр ЮУрГУ, 2013. - 131, [1] с. ил.

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

1. Галатенко, В.А. Основы информационной безопасности : курс лекций : учебное пособие / В.А. Галатенко. – Издание 2-е, исправленное. – М. : ИНТУИТ.РУ "Интернет-университет Информационных Технологий", 2004. – 264 с.
2. Скляров, Д.В. Искусство защиты и взлома информации / Д.В. Скляров. – СПб. : БХВ-Петербург, 2004. – 288 с.
3. Столлингс, В. Криптография и защита сетей: принципы и практика : пер. с англ. / В. Столлингс. – 2-е изд.. – М. : Издательский дом "Вильямс", 2001. – 672 с.
4. Ховард, М. Защищённый код : пер. с англ. / М. Ховард, Д. Лебланк. – 2-е изд., испр. – М. : Издательско-торговый дом "Русская редакция", 2004. – 704 с.
5. Нортроп, Т. Разработка защищённых приложений на Visual Basic .NET и Visual C# .NET : учебный курс Microsoft / Т. Нортроп. – М. : Издательство "Русская редакция", 2007. – 688 с.
6. Яковлев, А.В. Криптографическая защита информации : учебное пособие / А.В. Яковлев [и др.]. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2006. – 140 с.
7. Харин, Ю.С. Математические и компьютерные основы криптологии : учебное пособие / Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. – Мн. : Новое знание, 2003. – 382 с.

г) методические указания для студентов по освоению дисциплины:

1. Переведенцев В.В. Методические указания по дисциплине "Основы безопасности IT-систем". Челябинск, ЮУрГУ. - 2022. - 12 стр.

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Переведенцев В.В. Методические указания по дисциплине "Основы безопасности IT-систем". Челябинск, ЮУрГУ. - 2022. - 12 стр.

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в	Библиографическое описание

		электронной форме	
1	Методические пособия для самостоятельной работы студента	Электронно-библиотечная система издательства Лань	Гошко, С.В. Технологии борьбы с компьютерными вирусами. Практическое пособие. [Электронный ресурс] — Электрон. дан. — М. : СОЛОН-Пресс, 2009. — 352 с. https://e.lanbook.com/book/13780
2	Основная литература	Электронно-библиотечная система издательства Лань	Климентьев, К.Е. Компьютерные вирусы и антивирусы: взгляд программиста. [Электронный ресурс] — Электрон. дан. — М. : ДМК Пресс, 2013. — 656 с. https://e.lanbook.com/book/100728
3	Дополнительная литература	Электронно-библиотечная система издательства Лань	Белов, Е.Б. Основы информационной безопасности. [Электронный ресурс] / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. — Электрон. дан. — М. : Горячая линия-Телеком, 2006. — 544 с. https://e.lanbook.com/book/5121
4	Основная литература	Электронно-библиотечная система издательства Лань	Курило, А.П. Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1. [Электронный ресурс] / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. — Электрон. дан. — М. : Горячая линия-Телеком, 2012. — 244 с. https://e.lanbook.com/book/5182
5	Дополнительная литература	Электронно-библиотечная система издательства Лань	Бирюков, А.А. Информационная безопасность: защита и нападение. [Электронный ресурс] — Электрон. дан. — М. : ДМК Пресс, 2012. — 474 с. https://e.lanbook.com/book/50578
6	Основная литература	Электронно-библиотечная система издательства Лань	Шаньгин, В.Ф. Информационная безопасность. [Электронный ресурс] — Электрон. дан. — М. : ДМК Пресс, 2014. — 702 с. https://e.lanbook.com/book/50578

Перечень используемого программного обеспечения:

1. Microsoft-Windows(бессрочно)
2. Microsoft-Office(бессрочно)
3. ФГАОУ ВО "ЮУрГУ (НИУ)"-Портал "Электронный ЮУрГУ" (https://edu.susu.ru)(бессрочно)
4. -Oracle VM VirtualBox(бессрочно)

Перечень используемых профессиональных баз данных и информационных справочных систем:

1. ООО "ГарантУралСервис"-Гарант(бессрочно)

8. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Практические занятия	115	Проектор, Компьютерная техника с предустановленным

и семинары	(3б)	программным обеспечением
Самостоятельная работа студента	115 (3б)	Проектор, Компьютерная техника с предустановленным программным обеспечением
Зачет,диф.зачет	115 (3б)	Проектор, Компьютерная техника с предустановленным программным обеспечением
Лекции	115 (3б)	Проектор, Компьютерная техника с предустановленным программным обеспечением
Пересдача	115 (3б)	Проектор, Компьютерная техника с предустановленным программным обеспечением