УТВЕРЖДЕНО:
решением Ученого Совета ИЭ и Б
от « 23 » июня 2022г. Протокол № 09/252

Председатель _____Белый Е.М.
23 июня 2022г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	Обеспечение информационной безопасности организации
Факультет	Управления
Кафедра	Экономики и предпринимательства
Курс	1

Направление (специальность) 38.04.01 – «Экономика» (степень - магистр)
код направления (специальности), полное наименование

Профиль _«Экономическая безопасность организации»
_____
полное наименование

Форма обучения___заочная
очная, заочная, очно-заочная (указать только те, которые реализуются)

Дата введения в учебный процесс УлГУ: « 01 » сентября 2022 г.

Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20_____г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20_____г.

Сведения о разработчиках:

ФИО	Кафедра	Должность, ученая степень, звание
Сковиков А.Г.	Цифровой экономики	к.т.н., доцент

СОГЛАСОВАНО	СОГЛАСОВАНО
Заведующий кафедрой Э и П, реализующей дисциплину Белый Е.М.	Заведующий выпускающей кафедрой ЭБ, У и А Романова И.Б.
_ _____/___Белый Е.М._____/ *Подпись* *ФИО* «__23_»_____06_____2022_г.	_____/___Романова И.Б._____/ *Подпись* *ФИО* «__23_»_____06_____2022__г.

1. Цель и задачи освоения дисциплины

Дисциплина «Обеспечение информационной безопасности организации» посвящена изучению основ информационной безопасности. Рассматриваются основные понятия информационной безопасности, структура мер в области информационной безопасности, кратко описываются меры законодательного, административного, процедурного и программно-технического уровней. Излагаются взгляды на информацию, как объект защиты с выделением характерных свойств защищаемой информации. Рассматриваются виды угроз информационной безопасности; методы и средства борьбы с угрозами информационной безопасности; понятие политики безопасности, существующие типы политик безопасности; действующие стандарты информационной безопасности; нормативные руководящие документы.

Цель дисциплины – формирование у будущих специалистов и руководителей системных знаний по проблеме обеспечения комплексной защиты информационных ресурсов и управлению информационными рисками, а также практических навыков безопасной работы в информационных системах.

Задачи дисциплины:

- формирование системных представлений об управлении информационными рисками;
- изучение методов и средств комплексной защиты информации в информационных системах коммерческих предприятий и государственных учреждений;
- формирование практических навыков анализа защищенности информационных систем, использования встроенных возможностей ОС, MS Office, Брандмауэра Windows, Internet Explorer, а также антивирусных и криптографических средств для обеспечения безопасности информации;
- получение теоретических знаний и практических навыков при решении типовых задач по обеспечению информационной безопасности;
- освоение типовых методов и средствв предотвращения и ликвидации ущерба, который может быть нанесен организации при реализации различных угроз информационной безопасности;
- освоение типовых информационных процессов, реализуемых в организации при решении различных управленческих задач;
- определение основных угроз информационной безопасности, возникающих в процессе функционирования организации;
- формирование навыков использования полученных знаний для правильного выбора решений при разработке криптографических, организационных, технических средств защиты информации.

В результате изучения курса студенты должны ознакомиться с методикой и инструментами построения комплексной, эшелонированной системы информационной безопасности. То есть, дисциплина направлена на изучение основных теоретических положений и методов, формирование умений и привитие навыков применения теоретических знаний для решения прикладных задач, а также развитие новых подходов к обеспечению информационной безопасности в сфере экономики.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Обеспечение информационной безопасности организации» принадлежит вариативной части Блока Б1 «Дисциплины (модули)» основной профессиональной образовательной программы (ОПОП) и является дисциплиной по выбору. Она является одной из основополагающих дисциплин в системе подготовки магистров по направлению 38.04.01 – «Экономика». Вместе с другими курсами, посвященными трендам трансформа-

ции современной экономики, дисциплина «Информационная безопасность» составляет основу образования специалиста в части ОПОП, касающейся современных тенденций становления и развития информационного общества. Она охватывает широкий круг проблем и поэтому связана со многими дисциплинами, которые преподают в рамках изучения современных информационных технологий, т.к. ее цель – получение студентом знаний, умений и навыков обеспечения информационной безопасности. Цифровая трансформация помогает не просто следовать тенденции, но и экономить время, деньги, ресурсы, то есть оставаться конкурентоспособными. Современные коммуникационные технологии помогают реализовать широкий набор бизнес-процессов предприятий и организаций различных видов деятельности, размеров и организационно-правовых форм. Общие тенденции информатизации экономики таковы, что информационные системы, обеспечивающие взаимодействие предприятия с другими субъектами хозяйственной деятельности, и их реализация на микроуровне становятся неразрывными, поэтому требования к уровню подготовки экономиста в области информационной безопасности постоянно повышаются. Информационная безопасность является важнейшей составляющей частью общей интегральной или комплексной безопасности, причем на любом возможном уровне рассмотрения – национальном, региональном, отраслевом, корпоративном и даже персональном. При этом информационная безопасность обладает специфической особенностью. При анализе необходимо учитывать, что сервисы защиты информации являются неотъемлемой частью информационных технологий, которые в настоящее время развиваются доселе невиданными темпами. Чтобы не отставать от технического прогресса, необходимо не просто внедрить некоторые готовые инструменты в сфере информационной безопасности, а разработать методологию генерации новых решений, отвечающих современному состоянию дел, а в идеале – работающих на перспективу.

В рамках дисциплины изучаются основные направления развития современных информационных технологий и обеспечения безопасности информационных систем. Шифр дисциплины в рабочем учебном плане - Б1.В.ДВ.04.02.

Дисциплина рассчитана на обучающихся, имеющих подготовку по предшествующим курсам, касающихся информатики, вычислительной техники, статистики, алгебры и теории чисел, теории вероятности. Обучающиеся должны иметь подготовку (знания, умения, навыки и компетенции) в области информатики, информационных технологий и систем, глобальных сетей, организации и инфраструктуры предпринимательской деятельности, производственных и бизнес-процессов. Для изучения основных разделов дисциплины студенты должны обладать компетенциями, развиваемыми в рамках дисциплин, касающихся основ теории, прикладной математики, информационных технологий. Помимо этого, для успешного освоения данного курса обучающиеся должны иметь навык самостоятельной работы с различными источниками информации (интернет, печатные издания), уметь обобщать информацию, полученную из разных источников, представлять результаты своих исследований.

Дисциплина «Обеспечение информационной безопасности организации» реализуется в одном семестре с дисциплинами: Правовые основы обеспечения экономической безопасности; Экономическая безопасность организации; Национальная и региональная экономическая безопасность.

Постреквизиты. Прохождение данной дисциплины предшествует прохождению: следующих дисциплин:

- Цифровая экономика;
- Стратегический анализ и прогнозирование;
- Анализ отраслевых рынков и конкурентная политика;
- Налоговое планирование и администрирование;
- Оптимизация налогообложения;

- Эконометрика;
- Технологическая безопасность;
- Кадровая безопасность компании;
- Кадровое обеспечение предприятия;
- Мониторинг и диагностика экономической безопасности;
- Финансовый консалтинг;
- Управление инвестиционными проектами;
- Финансовая безопасность организации;
- Практика по профилю профессиональной деятельности;
- Экономическая теория (продвинутый курс);
- Контроллинг и управленческий учет на предприятии;
- Управление затратами.

Знания, навыки и умения, приобретенные в результате прохождения курса, также будут востребованы при прохождении практик, осуществлении проектной деятельности, выполнении курсовых и выпускной квалификационной работ, связанных с обеспечением защиты информационных систем, ИТ-инфраструктуры, безопасной работы в сети Интернет, в процессе подготовки к сдаче и сдачи государственного экзамена, защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

3. Перечень планируемых результатов освоения дисциплины

Код компетенции	**Формулировка компетенции**	**Код индикатора компетенции**	**Индикаторы достижения компетенции**
ПК-1	Способен к организации и контролю экономической безопасности организации	ИД-1пк1	***знать:*** ИД-1пк1 - типовые цифровые технологии проведения анализа и разработки управленческих решений в сфере информационной безопасности организации; ИД-1.1пк1 - основные понятия информационной безопасности.
		ИД-2пк1	***уметь:*** ИД-2пк1 - использовать безопасные информационные технологии в своей профессиональной деятельности; ИД-2.1пк1 - формировать информационную базу для разработки решений в сфере информационной безопасности организации.
		ИД-3пк1	***владеть:*** ИД-3пк1

			- навыками обеспечения безопасной работы на компьютере; ИД-3.1пк1 - навыками безопасного поиска информации в глобальной информационной сети Интернет.
ПК-4	Способен управлять рисками в области обеспечения экономической безопасности организации	ИД-1пк4	***знать:*** ИД-1пк4 - основные угрозы и способы классификации угроз информационной безопасности; ИД-1.1пк4 - технологические возможности злоумышленников по преодолению систем защиты информации.
		ИД-2пк4	***уметь:*** ИД-2пк4 - анализировать информационную безопасность многопользовательских систем ИД-2.1пк4 - видеть конкретную ситуацию, прогнозировать и предвидеть, рассчитывать риски, ставить цели и задачи в области информационной безопасности.
		ИД-3пк4	***владеть:*** ИД-3пк4 - методами обеспечения информационной безопасности жизненного цикла информационного контента предприятия и Интернет-ресурсов.

4. ОБЪЕМ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачётных единицах (всего) - 2 ЗЕТ

4.2. Объем дисциплины по видам учебной работы (в часах) 72ч.

Вид учебной работы	Количество часов (форма обучения заочная)			
	Всего по плану	В т.ч. по семестрам		
		1	2	3
1	**2**	**3**	**4**	**5**
Контактная работа обучающихся с преподавателем в соот-	10	10*		

ветствии с УП				
Аудиторные занятия:	10	10*		
лекции	4	4*		
семинары и практические занятия	6	6*		
лабораторные работы, практикумы	-	-		
Самостоятельная работа	58	58		
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др.(не менее 2 видов)	Тестирование, реферат	Тестирование, реферат		
Курсовая работа	-	-		
Контроль	4	4		
Виды промежуточной аттестации (экзамен, зачет)	Зачет	Зачет		
Всего часов по дисциплине	72	72		

* работы ППС с обучающимися для проведения занятий в дистанционном формате с применением электронного обучения

4.3. Содержание дисциплины (модуля) Распределение часов по темам и видам учебной работы:

Форма обучения: заочная

В результате освоения данного курса у магистранта должна быть сформирована парадигма рационального управления организацией как совокупностью технологических процессов обработки информации, с учетом ценности информации различного содержания, которая циркулирует по каналам связи в организации и пересылается партнерам организации по экономической деятельности во внешней среде, критерием рациональности задач управления, так или иначе рассматриваемых в рамках курса, является минимизация

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
1. Основные понятия информационной безопасности.	13	1	2			10	устный опрос, дискуссия по теме

Жизненный цикл контента. платформы для эффективной корпоративной работы.							занятия, экзамен
2. Риски в сфере информационной безопасности в организации.	11	1				10	тестирование, устный опрос, реферат, зачет
3. ITIL/ITSM – концептуальная основа процессов IT – службы. Решения Hewlett-Packard по управлению информационными системами. Решения IBM по управлению информационными системами.	10					10	тестирование, устный опрос, реферат, экзамен
4. Повышение эффективности IT-инфраструктуры предприятия. технология Microsoft обеспечения информационной безопасности.	11	1				10	тестирование, устный опрос, реферат, экзамен
5. Программно-технические средства обеспечения информационной безопасности.	23	1	4		6	18	тестирование, устный опрос, реферат, экзамен
Итого	**68**	**4**	**6**		**6**	**58**	
контроль	4						
Всего	**72**	**4**	**6**		**6**	**58**	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (Модуля)

Тема 1. Основные понятия информационной безопасности. Жизненный цикл контента. платформы для эффективной корпоративной работы.

Основные понятия: задачи, объект, предмет, методы информационной безопасности. Политика в сфере обеспечения информационной безопасности России. Концептуальная модель информационной безопасности. Официальные органы, обеспечивающие информационную безопасность в Российской Федерации. Обзор российского законодательства в сфере информационных технологий. Федеральный закон «Об информации, информационных технологиях и о защите информации», законодательство РФ в сфере СМИ. Федеральный закон «О государственной тайне». Федеральный закон «О персональных данных». Федеральный закон «Об электронной подписи». Правовое обеспечение информационной безопасности. Доктрина информационной безопасности РФ и Стратегия национальной безопасности Российской Федерации до 2020 года. Составляющие концептуальной модели информационной безопасности. Современная концепция информационной безопасности. Цели защиты информации. Носители защищаемой информации. Понятие информации. Сведения и данные, отличие от информации. Информация по уровню доступа. Конфиденциальность информации. Понятие конфиденциальной информации. Классификация конфиденциальной информации. Понятие государственной тайны. Степени грифа секретности. Виды сведений составляющих государственную тайну. Перечень информации, не подлежащей к засекречиванию. Классификация видов профессиональной тайны и объекты их приложения. Информационная система организации. Иерархичность систем управления. Принятие решений и процесс принятия Решений. Задача информационной системы. Создание, сбор, проверка, утверждение, публикация, распространение и архивирование. Бизнес-процессы с неизменяемым контентом. Модели контента: реляционная модель, объектно-ориентированная модель, онтологическая модель. Основы построения понятийного аппарата информационных ресурсов. Программные и инструментальные средства обеспечения процессов жизненного цикла контента. Распространение контента. Регистрация и аутентификация пользователей. Управление доступом к корпоративному контенту. Персонализация и кастомизация пользователей свободно распространяемого контента. Организация взаимодействия пользователей контента. Распределенное управление контентом. Управление процессами коллективной работы по созданию контента. Системы управления контентом. Сервисы управление контентом. Базовые системные сервисы. Статистические контентные сервисы. Интерактивные сервисы. Административные сервисы. Виды классификации контента. Классификация контента в задачах информационного обеспечения: архивирование контента, соблюдение нормативных требований, управление электронной почтой, управление контентно-ориентированными бизнес-процессами, управление таксономией, обработка запросов, поддержка контактов, онлайновая поддержка пользователей. Классификация контента в рамках внутренних и внешних таксономий. Сервисы классификации для контент-ориентированных приложений. Системы управления веб-контентом. (WCMS). Типовые функции управления веб-сайтом. Добавление и изменений информации. Изменение структуры сайта. Изменение дизайна сайта. Возможность использования шаблонных типов данных. Обеспечение работы с содержанием и визуальным отображением страниц. Регистрация и аутентификация пользователей. Персонализация. Состав требований к системе управления веб-контентом. Критерии оценки системы управления веб-контентом. Системы электронного документооборота предприятия, использующие веб-интерфейс. Принципы интеграции систем управления контентом предприятия (Enterprise Content Management - ECM) с системами управления бизнес-процессами предприятия (Business Process Management - BPM). Основные компоненты ECM. Управление документами: регистрация, контроль версий, безопасность, катологизация. Управление веб-контентом: автоматизация процессов веб-администрирования, управление динамическим контентом и взаимодействие с пользова-

телями. Управление записями. Управление движением и преобразованием в электронный вид бумажных документов. Документальная поддержка бизнес-процессов.

Тема 2. Риски в сфере информационной безопасности в организации.

Риски в сфере информационной безопасности в организации. Основные угрозы информационной безопасности в организации: нарушения целостности, нарушения конфиденциальности и нарушения доступности информации. Основные причины нарушения информационной безопасности и источники угроз информационной безопасности в зависимости от формы представления информации и применяемых технологий обработки. Понятие угроз безопасности. Классификация угроз информационной безопасности. Основная классификация угроз: угрозы нарушения конфиденциальности информации, угрозы нарушения целостности информации, угрозы нарушения доступности информации. Методы перечисления угроз. Случайные и преднамеренные угрозы. Технологические возможности злоумышленников по преодолению систем защиты информации. Признаки угрозы безопасности информации в распределенных вычислительных системах (РВС): по характеру воздействия; по цели воздействия; по условию начала осуществления воздействия; по наличию обратной связи с атакуемым объектом; по расположению субъекта атаки относительно атакуемого объекта; по уровню эталонной модели ISO/OSI, на котором осуществляется воздействие. Характеристика и механизмы реализации типовых удаленных атак. Понятие типовой удаленной атаки. Анализ сетевого трафика. Подмена доверенного объекта или субъекта РВС. Ложный объект РВС. Внедрение в РВС ложного объекта путем навязывания ложного маршрута. Внедрение в РВС ложного объекта путем использования недостатков алгоритмов удаленного поиска. Использование ложного объекта для организации удаленной атаки на РВС. Селекция потока информации и сохранение ее на ложном объекте РВС. Модификация информации. Подмена информации. Отказ в обслуживании. Понятие несанкционированного доступа (НСД). Направления защиты от НСД. Основные способы НСД. Принципы защиты от НСД. Классификация нарушителей. Понятие системы разграничения доступа (СРД). Основные функции СРД.

Тема 3. ITIL/ITSM − концептуальная основа процессов IT –службы. Решения Hewlett-Packard по управлению информационными системами. Решения IBM по управлению информационными системами.

Общие сведения о библиотеке ITIL. Модель ITSM. Процессы поддержки ИТ-сервисов: управление инцидентами; управление проблемами; управление конфигурациями; управление изменениями; управление релизами. Процессы предоставления ИТ-сервисов: процесс управления уровнем сервиса; процесс управления мощностью; процесс управления доступностью; процесс управления непрерывностью; процесс управления финансами; процесс управления безопасностью. Соглашение об уровне сервиса. Модель информационных процессов ITSM Reference Model; программные решения HP OpenView; управление бизнесом; управление приложениями; управление ИТ-службой. Управление идентификацией – Identity Management; решение HP OpenView Service Desk; управление ИТ-инфраструктурой; управление ИТ-ресурсами. Методологическая основа построения управляемых ИС. Инструментарий управления ИТ-инфраструктурой. Microsoft System Management Server 2012, System Center Reporting Manager 2012, Microsoft System Center Data Protection Manager 2012, Microsoft System Center Capacity Planner 2012.

Тема 4. Повышение эффективности IT-инфраструктуры предприятия. технология Microsoft обеспечения информационной безопасности.

Уровни зрелости ИТ-инфраструктуры предприятия. Методология Microsoft по эксплуатации ИС. Групповые политики. Безопасный доступ в сеть. Аутентификация пользо-

вателей. Защита коммуникаций. Защита от вторжений и вредоносного ПО. Безопасность мобильных пользователей корпоративных систем. Службы терминалов. Защита данных. Exchange Server 2016. Технология Microsoft SharePoint. Интеграция приложений Microsoft Office с технологиями SharePoint. Microsoft Office InfoPath 2016. Служба управления правами Windows. Система управления правами на доступ к информации в Office 2016. Эффективное взаимодействие в режиме реального времени. Live Communications Server 2016. Microsoft Office Live Meeting 2016.

Тема 5. Программно-технические средства обеспечения информационной безопасности.

Техническое обеспечение информационной безопасности. Понятие сервиса безопасности. Понятие архитектурной безопасности. Классификация сервисов безопасности. Средства идентификации и аутентификации пользователей. Идентификация и аутентификация, управление доступом. Парольная аутентификация. Одноразовые пароли. Система S/KEY компании Bellcore. Сервер аутентификации Kerberos. Идентификация/аутентификация с помощью биометрических данных. Управление доступом. Матрица доступа. Произвольное (или дискреционное) управление доступом. Принудительное (мандатное) управление доступом. Списки управления доступом. Ограничивающий интерфейс. Ролевое управление доступом. Статическое разделение обязанностей. Динамическое разделение обязанностей. Основные понятия и классификация средств криптографической защиты информации. Криптографические методы защиты информации. Методы стеганографии. Аппаратно-программные средства защиты информации: средства обеспечения конфиденциальности данных; средства аутентификации электронных данных и средства управления ключевой информацией. Классификация методов шифрования. Требования к современным шифрам. Методы симметричного шифрования. Блочное и потоковое шифрование. Классическая сеть Фейстеля. Алгоритм шифрования DES и его модификации. Абсолютно надежный шифр. Основные свойства симметричных криптосистем. Основные свойства асимметричных криптосистем. Генерация и хранение ключей. Распределение ключей. Управление ключами в системах с открытым ключом. Алгоритм Диффи-Хелмана. Основные свойства хэш-функций. Основные свойства цифровой подписи. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамаля. Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-94. Схемы слепой подписи. Схемы неоспоримой подписи. Защита информации при работе в сети Интернет. Протоколирование и аудит, их место в общей архитектуре безопасности. Активный аудит. Подозрительная активность. Сигнатура атаки. Функциональные компоненты, входящие в состав средств активного аудита. Применение аудита в ОС семейства Windows для отслеживания деятельности пользователей. Настройка политики аудита. Понятие демилитаризованной зоны. Механизмы защиты, реализуемые межсетевым экраном (МЭ): фильтрация сетевого трафика; шифрование (создание VPN); трансляция адресов; аутентификация (дополнительная); противодействие некоторым сетевым атакам (наиболее распространённым); управление списками доступа на маршрутизаторах. Типы МЭ. Пакетные фильтры. Шлюзы уровня соединения. Шлюзы прикладного уровня. Технологии Proxy и Stateful inspection. Концепция построения защищённых виртуальных частных сетей VPN. Функции и компоненты сети VPN. VPN решения для построения защищённых корпоративных сетей. Два вида средств поддержания высокой доступности: обеспечение отказоустойчивости (нейтрализация отказов, живучесть) и обеспечение безопасного и быстрого восстановления после отказов (обслуживаемость). Классификация компьютерных вирусов и вредоносных программ. Файловые, загрузочные и сетевые вирусы. Методы и средства борьбы с вирусами и вредоносными программами. Профилактика заражения вирусами компьютерных систем и порядок действий пользователей в случае заражения.

Механизмы распространения вирусов. Каналы распространения вирусов. Классические компьютерные вирусы. Макровирусы. Троянские программы. Сетевые черви. Антивирусное ПО. Обнаружение компьютерных вирусов. Комплексная система защиты информации.

Лекционный курс предполагает систематизированное изложение основных вопросов учебной дисциплины и должен давать наибольший объем информации и обеспечивать более глубокое понимание учебных вопросов при значительно меньших затратах времени, чем это требуется большинству студентов на самостоятельное изучение материала.

Методические рекомендации при работе над конспектом лекций во время проведения лекции

В ходе лекционных занятий вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

В ходе подготовки к практическим занятиям изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д. При этом учесть рекомендации преподавателя и требования учебной программы. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной учебной программой. Подготовить тезисы для выступлений по всем учебным вопросам, представляющим интерес. Готовясь к докладу или реферативному сообщению, обращаться за методической помощью к преподавателю. Составить план-конспект своего выступления. Продумать примеры с целью обеспечения тесной связи изучаемой теории с реальной жизнью. Своевременное и качественное выполнение самостоятельной работы базируется на соблюдении настоящих рекомендаций и изучении рекомендованной литературы. Студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании курсовых и дипломных работ.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

– семинар, дискуссия.

№ п/п	№ темы	Тема семинара	Форма проведения	Кол-во часов
1	2	Характеристика и механизмы реализации типовых удаленных атак. Понятие типовой удаленной атаки. Анализ сетевого трафика. Подмена доверенного объекта или субъекта РВС. Ложный объект РВС. Внедрение в РВС ложного объекта путем навязывания ложного маршрута. Внедрение в РВС ложного объекта путем использования недостатков алгоритмов удаленного по-	семинар, дискуссия	2

		иска. Использование ложного объекта для организации удаленной атаки на РВС. Селекция потока информации и сохранение ее на ложном объекте РВС. Модификация информации. Подмена информации. Отказ в обслуживании.		
2	5	Классическая сеть Фейстеля. Алгоритм шифрования DES и его модификации. Генерация и хранение ключей. Распределение ключей. Управление ключами в системах с открытым ключом. Алгоритм Диффи-Хелмана. Основные свойства цифровой подписи. Алгоритм цифровой подписи RSA. Алгоритм цифровой подписи Эль Гамаля. Алгоритм цифровой подписи DSA. Троянские программы. Сетевые черви. Антивирусное ПО. Обнаружение компьютерных вирусов. Комплексная система защиты информации.	семинар, дискуссия	2
3	5	Механизмы защиты, реализуемые межсетевым экраном (МЭ): фильтрация сетевого трафика; шифрование (создание VPN); трансляция адресов; аутентификация (дополнительная); противодействие некоторым сетевым атакам; управление списками доступа на маршрутизаторах. Типы межсетевых экранов. Пакетные фильтры. Шлюзы уровня соединения. Stateful Inspection firewall. Host-based firewall. Примеры правил. Персональные firewall и персональные устройства firewall. Шлюзы прикладного уровня. Прокси-сервер прикладного уровня. Выделенные прокси-серверы. Примеры правил. Трансляция сетевых адресов (NAT). Концепция построения защищённых виртуальных частных сетей VPN. Функции и компоненты сети VPN. VPN решения для построения защищённых корпоративных сетей.	семинар, дискуссия	2
		Итого:		**6**

ТЕМА 2. РИСКИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ

ЗАНЯТИЕ 1

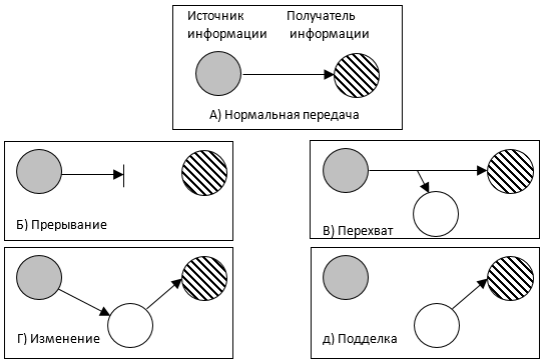
Типовые удаленные атаки. Примеры типовых удаленных атак

Форма проведения – семинар, дискуссия.

Вопросы по теме (для обсуждения на занятии, для самостоятельного изучения).

1. Категории информации.

2. Удаленные атаки на распределенные вычислительные системы.



3. Характеристика и механизмы реализации типовых удаленных атак.
4. Понятие типовой удаленной атаки.
5. Анализ сетевого трафика.
6. Подмена доверенного объекта или субъекта РВС.
7. Ложный объект РВС.
8. Внедрение в РВС ложного объекта путем навязывания ложного маршрута.
9. Внедрение в РВС ложного объекта путем использования недостатков алгоритмов удаленного поиска.
10. Использование ложного объекта для организации удаленной атаки на РВС.
11. Селекция потока информации и сохранение ее на ложном объекте РВС.
12. Модификация информации.
13. Подмена информации.
14. Отказ в обслуживании.

ТЕМА 5. ПРОГРАММНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЗАНЯТИЕ 2

Примеры основных криптографических алгоритмов

Форма проведения – семинар, дискуссия, деловая игра.

Вопросы по теме (для обсуждения на занятии, для самостоятельного изучения).

1. Симметричные и ассиметричные криптосистемы.
2. Алгоритмы замены и перестановки.
3. Алгоритм шифрования DES и его модификации.
4. Генерация и хранение ключей.
5. Распределение ключей.

6. Управление ключами в системах с открытым ключом.
7. Алгоритм Диффи-Хелмана.
8. Основные свойства цифровой подписи.
9. Алгоритм цифровой подписи RSA.
10. Алгоритм цифровой подписи Эль Гамаля.
11. Алгоритм цифровой подписи DSA.
12. Категории вирусов.
13. Классические вирусы.
14. Макровирусы.
15. Троянские программы.
16. Сетевые черви.
17. Антивирусное ПО.
18. Обнаружение компьютерных вирусов.
19. Комплексная система защиты информации.

ЗАНЯТИЕ 3

Сервис информационной безопасности - Межсетевые экраны. Категории межсетевых экранов.

Форма проведения – семинар, дискуссия.

Вопросы по теме (для обсуждения на занятии, для самостоятельного изучения).

1. Механизмы защиты, реализуемые межсетевым экраном (МЭ): фильтрация сетевого трафика; шифрование (создание VPN); трансляция адресов; аутентификация (дополнительная); противодействие некоторым сетевым атакам.
2. Управление списками доступа на маршрутизаторах.
3. Типы межсетевых экранов.
4. Пакетные фильтры.
5. Шлюзы уровня соединения.
6. Stateful Inspection firewall.
7. Host-based firewall.
8. Примеры правил.
9. Персональные firewall и персональные устройства firewall.
10. Шлюзы прикладного уровня.
11. Прокси-сервер прикладного уровня.
12. Выделенные прокси-серверы.
13. Примеры правил.
14. Трансляция сетевых адресов (NAT).
15. Функции и компоненты сети VPN.
16. VPN решения для построения защищённых корпоративных сетей.

Практические (семинарские занятия) представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают основные разделы.

Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях. В обязанности преподавателя входят: оказание методической помощи и консультирование студентов по соответствующим темам курса.

На семинаре каждый его участник должен быть готовым к выступлению по всем поставленным в плане вопросам, проявлять максимальную активность при их рассмотрении. Выступление должно строиться свободно, убедительно и аргументировано. Препода-

ватель следит, чтобы выступление не сводилось к репродуктивному уровню (простому воспроизведению текста), не допускается и простое чтение конспекта. Необходимо, чтобы выступающий проявлял собственное отношение к тому, о чем он говорит, высказывал свое личное мнение, понимание, обосновывал его и мог сделать правильные выводы из сказанного. При этом студент может обращаться к записям конспекта и лекций, непосредственно к первоисточникам, использовать знание художественной литературы и искусства, факты и наблюдения современной жизни и т. д. Вокруг такого выступления могут разгореться споры, дискуссии, к участию в которых должен стремиться каждый. Преподавателю необходимо внимательно и критически слушать, подмечать особенное в суждениях студентов, улавливать недостатки и ошибки, корректировать их знания, и, если нужно, выступить в роли рефери, обратить внимание на то, что еще не было сказано, или поддержать и развить интересную мысль, высказанную выступающим студентом. В заключение преподаватель, как руководитель семинара, подводит итоги семинара. Он может (выборочно) проверить конспекты студентов и, если потребуется, внести в них исправления и дополнения.

Активность на практических занятиях оценивается по следующим критериям:

- ответы на вопросы, предлагаемые преподавателем;
- участие в дискуссиях;
- выполнение проектных и иных заданий;
- ассистирование преподавателю в проведении занятий.

Доклады и оппонирование докладов проверяют степень владения теоретическим материалом, а также корректность и строгость рассуждений.

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Данный вид работы не предусмотрен УП.

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Курсовые и контрольные работы не предусмотрены УП.

Реферат это одна из форм текущего контроля знаний и контроля самостоятельной работы. Реферат – это самостоятельная исследовательская работа, в которой автор раскрывает суть исследуемой проблемы; приводит различные точки зрения, а также собственные взгляды не нее. Содержание реферата должно быть логичным; изложение материала должно носить проблемно-тематический характер.

Цель реферата как формы текущего контроля знаний и контроля самостоятельной работы - стимулировать раскрытие исследовательского потенциала учащегося, способность к творческому поиску, сотрудничеству, самораскрытию и проявлению возможностей.

Примерная тематика рефератов:

№ задания	Тема
1	Информация как источник данных.
2	Классификация информации. Виды данных и носителей.
3	Ценность информации. Цена информации.
4	Количество и качество информации.
5	Основные виды информационных ресурсов организации: данные, информация и знания.
6	Свойства информации.
7	Понятие документированных, электронных и недокументированных информационных ресурсов.

8	Право на доступ к информации.
9	Критерии оценки информации: систематичность, естественность и возможность повторного использования.
10	Роль и значение информационных ресурсов в информатизации общества.
11	Паспорт информационного ресурса.
12	Технологии управления информационными ресурсами.
13	Понятие информационной системы.
14	Особенности и эволюция информационных систем.
15	Закон «Об информации, информационных технологиях и о защите информации».
16	Эволюция изменений технологии и бизнес-условий. Смена парадигм в управлении документами: от бумажных документов к электронным, использование Интернет-публикаций.
17	Методы несанкционированного доступа к информации.
18	Основные способы привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.
19	Способы наблюдения с использованием технических средств.
20	Каналы утечки информации. Технические каналы утечки
21	Классификация технических каналов утечки по физической природе носителя.
22	Классификация технических каналов утечки по информативности.
23	Классификация технических каналов утечки по времени функционирования.
24	Классификация технических каналов утечки по структуре.
25	Наблюдение в оптическом диапазоне и применяемые для этого средства. Характеристики таких средств.
26	Перехват электромагнитных излучений.
27	Акустическое подслушивание. Эффекты, возникающие при подслушивании.
28	Понятия скрытия информации, виды скрытий. Информационный портрет.
29	Противодействие наблюдению. Способы маскировки.
30	Способы и средства противодействия подслушиванию.
31	Нейтрализация закладных устройств.
32	Состав инженерной защиты и технической охраны объектов.
33	Инженерные конструкции и сооружения для защиты информации. Их классификация.
34	Средства идентификации личности.
35	Классификация датчиков охранной сигнализации.
36	Классификация извещателей.
37	Телевизионные системы наблюдения.
38	Основные средства системы видеоконтроля.
39	Защита личности как носителя информации.
40	Системный подход к защите информации.
41	Параметры системы защиты информации.
42	Этапы проектирования системы защиты информации.
43	Потенциальные каналы утечки информации.
44	Этапы разработки мер по предотвращению угроз утечки информации.
45	Понятие информационной безопасности. Информационная безопасность личности, общества и государства. Конфиденциальная информация.
46	Категории информационной безопасности в КС. Классификация угроз.

47	Общая характеристика угроз доступности.
48	Общая характеристика угроз целостности.
49	Общая характеристика угроз конфиденциальности.
50	Обобщенные модели системы защиты информации в КС. Одноуровневые и многоуровневые модели. Общая характеристика средств и методов защиты информации в КС.
51	Общая характеристика организационных мероприятий, обеспечивающих информационную безопасность КС. Основные задачи службы безопасности.
52	Содержательный смысл понятия комплексной системы защиты информации (КСЗИ) в компьютерных системах. Основные принципы и положения, реализующие системный подход к построению КСЗИ.
53	Отечественное законодательство в области информации и защиты информации.
54	Минимизация ущерба, наносимого КС авариями и стихийными бедствиями. Дублирование информации. Технология RAID. Резервирование технических средств.
55	Общая характеристика технических каналов утечки информации в КС.
56	Базовые принципы, лежащие в основе моделей политики безопасности в КС. Матричная (дискреционная) модель и мандатная (полномочная) модель управления доступом к ресурсам КС.
57	Средства и методы разграничения доступа к ресурсам КС.
58	Защита программных средств КС от несанкционированного копирования и исследования.
59	Общие понятия, история развития и классификация криптографических средств.
60	Как характеризуется роль ИС-службы в современном бизнесе?
61	Чем модель ITSM отличается от традиционного функционального подхода к организации ИТ-службы?
62	Перечислите особенности проекта ITIL?
63	Какие направления управления ИТ-услугами описаны в проекте ITIL Refresh?
64	Какие процессы включены в блок поддержки ИТ-сервисов?
65	Какие процессы включены в блок предоставления ИТ-сервисов?
66	Поясните назначение процесса управления инцидентами.
67	Назначение библиотеки эталонного ПО - DSL.

Формулировки приведенных выше тем являются примерными и могут быть изменены. Изменения согласуются с преподавателем, ведущим дисциплину. Кроме этого, обучающиеся могут предлагать собственные темы для исследования. Инициативные темы также согласуются с преподавателем.

В процессе изучения курса каждый должен подготовить реферат, который будет засчитан преподавателем, ведущим дисциплину.

Оценивая реферат, преподаватель обращает внимание на:

- соответствие содержания выбранной теме;
- отсутствие в тексте отступлений от темы;
- соблюдение структуры работы, четкость изложения и обоснованность выводов;
- умение работать с научной литературой - вычленять проблему из контекста;
- умение логически мыслить;
- культуру письменной речи;

- умение оформлять научный текст (правильное применение и оформление ссылок, составление библиографии и т.д.);
- умение правильно понять позицию авторов, работы которых использовались при написании реферата;
- способность верно, без искажения передать используемый авторский материал;
- соблюдение объема работы;
- соответствие установленным правилам оформления работы;
- аккуратность и правильность технического выполнения работы.

Требования к оформлению и содержанию письменной работы содержатся в «Методических рекомендациях по написанию реферата».

9.ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

Индекс компетенции	№ задания	Формулировка вопроса
ПК-1	1	Информация как источник данных.
ПК-1	2	Классификация информации. Виды данных и носителей.
ПК-1	3	Ценность информации. Цена информации.
ПК-1	4	Количество и качество информации.
ПК-1	5	Основные виды информационных ресурсов организации: данные, информация и знания.
ПК-1	6	Свойства информации.
ПК-1	7	Понятие документированных, электронных и недокументированных информационных ресурсов.
ПК-1	8	Право на доступ к информации.
ПК-1	9	Критерии оценки информации: систематичность, естественность и возможность повторного использования.
ПК-1	10	Роль и значение информационных ресурсов в информатизации общества.
ПК-1	11	Паспорт информационного ресурса.
ПК-1	12	Технологии управления информационными ресурсами.
ПК-4	13	Понятие информационной системы.
ПК-4	14	Особенности и эволюция информационных систем.
ПК-4	15	Закон «Об информации, информационных технологиях и о защите информации».
ПК-4	16	Эволюция изменений технологии и бизнес-условий. Смена парадигм в управлении документами: от бумажных документов к электронным, использование Интернет-публикаций.
ПК-4	17	Методы несанкционированного доступа к информации.
ПК-4	18	Основные способы привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации.
ПК-4	19	Способы наблюдения с использованием технических средств.
ПК-4	20	Каналы утечки информации. Технические каналы утечки
ПК-4	21	Классификация технических каналов утечки по физической природе носителя.
ПК-4	22	Классификация технических каналов утечки по информативности.

ПК-1	23	Классификация технических каналов утечки по времени функционирования.
ПК-1	24	Классификация технических каналов утечки по структуре.
ПК-1	25	Наблюдение в оптическом диапазоне и применяемые для этого средства. Характеристики таких средств.
ПК-1	26	Перехват электромагнитных излучений.
ПК-1	27	Акустическое подслушивание. Эффекты, возникающие при подслушивании.
ПК-1	28	Понятия скрытия информации, виды скрытий. Информационный портрет.
ПК-1	29	Противодействие наблюдению. Способы маскировки.
ПК-1	30	Способы и средства противодействия подслушиванию.
ПК-1	31	Нейтрализация закладных устройств.
ПК-1	32	Состав инженерной защиты и технической охраны объектов.
ПК-1	33	Инженерные конструкции и сооружения для защиты информации. Их классификация.
ПК-1	34	Средства идентификации личности.
ПК-1	35	Классификация датчиков охранной сигнализации.
ПК-1	36	Классификация извещателей.
ПК-1	37	Телевизионные системы наблюдения.
ПК-1	38	Основные средства системы видеоконтроля.
ПК-1	39	Защита личности как носителя информации.
ПК-4	40	Системный подход к защите информации.
ПК-4	41	Параметры системы защиты информации.
ПК-4	42	Этапы проектирования системы защиты информации.
ПК-4	43	Потенциальные каналы утечки информации.
ПК-4	44	Этапы разработки мер по предотвращению угроз утечки информации.
ПК-4	45	Понятие информационной безопасности. Информационная безопасность личности, общества и государства. Конфиденциальная информация.
ПК-4	46	Категории информационной безопасности в КС. Классификация угроз.
ПК-4	47	Общая характеристика угроз доступности.
ПК-4	48	Общая характеристика угроз целостности.
ПК-4	49	Общая характеристика угроз конфиденциальности.
ПК-4	50	Обобщенные модели системы защиты информации в КС. Одноуровневые и многоуровневые модели. Общая характеристика средств и методов защиты информации в КС.
ПК-4	51	Общая характеристика организационных мероприятий, обеспечивающих информационную безопасность КС. Основные задачи службы безопасности.
ПК-4	52	Содержательный смысл понятия комплексной системы защиты информации (КСЗИ) в компьютерных системах. Основные принципы и положения, реализующие системный подход к построению КСЗИ.
ПК-4	53	Отечественное законодательство в области информации и защиты информации.

ПК-1	54	Минимизация ущерба, наносимого КС авариями и стихийными бедствиями. Дублирование информации. Технология RAID. Резервирование технических средств.
ПК-1	55	Общая характеристика технических каналов утечки информации в КС.
ПК-1	56	Базовые принципы, лежащие в основе моделей политики безопасности в КС. Матричная (дискреционная) модель и мандатная (полномочная) модель управления доступом к ресурсам КС.
ПК-1	57	Средства и методы разграничения доступа к ресурсам КС.
ПК-1	58	Защита программных средств КС от несанкционированного копирования и исследования.
ПК-1	59	Общие понятия, история развития и классификация криптографических средств.
ПК-1	60	Как характеризуется роль ИС-службы в современном бизнесе?
ПК-1	61	Чем модель ITSM отличается от традиционного функционального подхода к организации ИТ-службы?
ПК-1	62	Перечислите особенности проекта ITIL?
ПК-1	63	Какие направления управления ИТ-услугами описаны в проекте ITIL Refresh?
ПК-1	64	Какие процессы включены в блок поддержки ИТ-сервисов?
ПК-1	65	Какие процессы включены в блок предоставления ИТ-сервисов?
ПК-1	66	Поясните назначение процесса управления инцидентами.
ПК-1	67	Назначение библиотеки эталонного ПО - DSL.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Содержание, требования, условия и порядок организации самостоятельной работы обучающихся с учетом формы обучения определяются в соответствии с «Положением об организации самостоятельной работы обучающихся», утвержденным Ученым советом УлГУ (протокол №8/268 от 26.03.2019 г.).

Форма обучения – *заочная*.

Название разделов и тем	**Вид самостоятельной работы** *(проработка учебного материала, решение задач, реферат, доклад, контрольная работа, подготовка к сдаче зачета, экзамена и др.)*	**Объем в часах**	**Форма контроля** (*проверка решения задач, реферата и др.)*
1. Основные понятия информационной безопасности. Жизненный цикл контента. платформы для эффективной корпоративной работы.	• Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины; • Подготовка к тестированию; Подготовка к сдаче экзамена	10	устный опрос, дискуссия по теме занятия, зачет
2. Риски в сфере информационной безопасности в организации.	• Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины;	10	тестирование, устный опрос, реферат, зачет

	• Подготовка к тестированию; • Подготовка к сдаче экзамена		
3. ITIL/ITSM − концептуальная основа процессов IT –службы. Решения Hewlett-Packard по управлению информационными системами. Решения IBM по управлению информационными системами.	• Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины; • Подготовка к тестированию; • Подготовка к сдаче экзамена	10	тестирование, устный опрос, реферат, зачет
4. Повышение эффективности IT-инфраструктуры предприятия. технология Microsoft обеспечения информационной безопасности.	• Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины; • Подготовка к тестированию; • Подготовка к сдаче экзамена	10	тестирование, устный опрос, реферат, зачет
5. Программно-технические средства обеспечения информационной безопасности.	• Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины; • Подготовка к тестированию; • Подготовка к сдаче экзамена	18	тестирование, устный опрос, реферат, зачет

Методические указания для обучающихся по освоению дисциплины

Для качественного усвоения студентами материала курса при выполнении ими индивидуальных заданий необходимо, чтобы все работы выполнялись студентами после проработки соответствующего лекционного материала. Основная задача по организации учебного процесса по данной дисциплине сводится к обеспечению равномерной активной работы студентов над курсом в течение всего учебного семестра. Студенты должны регулярно прорабатывать курс прослушанных лекций, готовиться к занятиям. Для контроля качества усвоения учебного материала студентами следует проводить опросы по изученной теме. Для долговременного запоминания изученного материала следует увязывать вновь изучаемые вопросы с материалом предыдущих тем, добиваться преемственности знаний.

При выполнении заданий, вынесенных на самостоятельное изучение, необходимо наряду с библиотечным фондом пользоваться различными источниками знаний, размещенными в сети Интернет.

При изучении данного курса студентам предстоит выполнить следующие виды работ:

- Анализ теоретического материала;
- Проработка лекционного материала;
- Выполнение практических заданий (лабораторные работы);
- Подготовка к тестированию.

Лекционные занятия

Лекционные занятия желательно проводить с применением демонстрационного материала – презентации лекций на ПК с проектором. С учетом современных возможностей, желательно обеспечивать слушателей раздаточным материалом на 1-2 лекции вперед. Материал этот должен носить иллюстративный характер (схемы, графики) и ни в коем случае не подменять конспекта, который слушатель должен составлять самостоятельно.

Практические занятия

На практических занятиях решаются задачи теоретического и прикладного характера, в том числе, выполняются лабораторные работы. После каждого практического занятия следует выдавать задание на самостоятельную работу, а на следующем занятии контролировать его выполнении. Также на практических занятиях следует проводить тестирование студентов.

Текущий контроль

Для текущего контроля успеваемости (по отдельным разделам дисциплины) и промежуточной аттестации используется компьютерное тестирование, проверка реферата.

1. Планирование и организация времени, необходимого для самостоятельного изучения дисциплины.

Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины:

- Изучение конспекта лекции в тот же день, после лекции: 30 минут- 1 час.
- Изучение конспекта лекции за день перед следующей лекцией: 30 минут- 1 час.
- Изучение теоретического материала по учебнику и конспекту: 1-2 часа в неделю.
- Подготовка к лабораторному занятию: 30 минут - 1 час.
- Изучение дополнительных источников, в том числе, в электронной форме: 1-2 часа в неделю.
- Всего в неделю: 1–3 часа.

2. Методические рекомендации по подготовке к практическим (лабораторным) занятиям.

По данному курсу предусмотрены лабораторные занятия. При подготовке к лабораторным занятиям следует изучить соответствующий теоретический материал по цифровой экономике, электронной коммерции, электронному бизнесу или электронным платежным системам. Теоретический материал курса становится более понятным, когда дополнительно к прослушиванию лекции и изучению конспекта, изучаются и книги по современным информационным технологиям.

Необходимо изучить лабораторную работу предыдущего занятия и выяснить те вопросы, которые показались непонятными.

Планы практических занятий, их тематика, рекомендуемая литература, цель и задачи ее изучения сообщаются преподавателем на вводных занятиях, в методических указаниях по данной дисциплине. Подготовка к практическому занятию включает 2 этапа: 1й - организационный; 2й - закрепление и углубление теоретических знаний. На первом этапе студент планирует свою самостоятельную работу, которая включает: - уяснение задания на самостоятельную работу; - подбор рекомендованной литературы; - составление плана работы, в котором определяются основные пункты предстоящей подготовки. Составление плана дисциплинирует и повышает организованность в работе. Второй этап включает непосредственную подготовку студента к занятию. Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы студент должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. Заканчивать подготовку следует составлением плана (конспекта) по изучаемому материалу (вопросу). Это позволяет составить

концентрированное, сжатое представление по изучаемым вопросам. В процессе подготовки к занятиям рекомендуется взаимное обсуждение материала, во время которого закрепляются знания, а также приобретается практика в изложении и разъяснении полученных знаний, развивается речь. При необходимости следует обращаться за консультацией к преподавателю. Идя на консультацию, необходимо хорошо продумать вопросы, которые требуют разъяснения. В начале занятия студенты под руководством преподавателя более глубоко осмысливают теоретические положения по теме занятия, раскрывают и объясняют основные положения публичного выступления. В процессе творческого обсуждения и дискуссии вырабатываются умения и навыки использовать приобретенные знания для различного рода ораторской деятельности. Записи имеют первостепенное значение для самостоятельной работы студентов. Они помогают понять построение изучаемого материала, выделить основные положения, проследить их логику и тем самым проникнуть в творческую лабораторию автора. Ведение записей способствует превращению чтения в активный процесс, мобилизует, наряду со зрительной, и моторную память. Следует помнить: у студента, систематически ведущего записи, создается свой индивидуальный фонд подсобных материалов для быстрого повторения прочитанного, для мобилизации накопленных знаний. Особенно важны и полезны записи тогда, когда в них находят отражение мысли, возникшие при самостоятельной работе. Важно развивать у студентов умение сопоставлять источники, продумывать изучаемый материал. Большое значение имеет совершенствование навыков конспектирования у студентов. Преподаватель может рекомендовать студентам следующие основные формы записи: план (простой и развернутый), выписки, тезисы. Результаты конспектирования могут быть представлены в различных формах. План - это схема прочитанного материала, краткий (или подробный) перечень вопросов, отражающих структуру и последовательность материала. Подробно составленный план вполне заменяет конспект. Конспект - это систематизированное, логичное изложение материала источника. Различаются четыре типа конспектов:

- План-конспект - это развернутый детализированный план, в котором достаточно подробные записи приводятся по тем пунктам плана, которые нуждаются в пояснении.
- Текстуальный конспект - это воспроизведение наиболее важных положений и фактов источника.
- Свободный конспект - это четко и кратко сформулированные (изложенные) основные положения в результате глубокого осмысливания материала. В нем могут присутствовать выписки, цитаты, тезисы; часть материала может быть представлена планом.
- Тематический конспект - составляется на основе изучения ряда источников и дает более или менее исчерпывающий ответ по какой-то схеме (вопросу).

3. Групповая консультация

Разъяснение является основным содержанием данной формы занятий, наиболее сложных вопросов изучаемого программного материала. Цель - максимальное приближение обучения к практическим интересам с учетом имеющейся информации и является результативным материалом закрепления знаний. Групповая консультация проводится в следующих случаях:

- когда необходимо подробно рассмотреть практические вопросы, которые были недостаточно освещены или совсем не освещены в процессе лекции;
- с целью оказания помощи в самостоятельной работе (написание рефератов, выполнение курсовых работ, сдача экзаменов, подготовка конференций);
- если студенты самостоятельно изучают нормативный, справочный материал, инструкции, положения.

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) основная литература

1. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — 342 с. — (Бакалавр и магистр. Модуль). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/441287
2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498844 (дата обращения: 29.05.2022).
3. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2019. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/433715

дополнительная литература

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/467370
2. Сковиков А.Г.Информационные технологии в управлении и экономике : учеб. пособие для студентов и аспирантов экон. профиля. Ч. 2 / Сковиков Анатолий Геннадьевич; УлГУ, ИЭиБ. - Ульяновск : УлГУ, 2016. - Загл. с экрана. - Электрон. текстовые дан. (1 файл : 4,91 МБ). - Текст : электронный. – URL: http://lib.ulsu.ru/MegaPro/Download/MObject/253

учебно-методическая

1. Сковиков А. Г.Методические указания для самостоятельной работы студентов по дисциплине «Обеспечение информационной безопасности организации» для магистрантов направления 38.04.01 «Экономика» (профиль «Экономическая безопасность организации») всех форм обучения / А. Г. Сковиков; УлГУ, ИЭиБ, Каф. цифровой экономики. - Ульяновск : УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 496 КБ). - Текст : электронный. – URL: http://lib.ulsu.ru/MegaPro/Download/MObject/6681

Согласовано:

б) программное обеспечение

Компьютерные программы:
Windows
Microsoft Office
Мой Офис Стандартный

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2022]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2022]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2022]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2022]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. ЭБС Znanium.com : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2022]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2022].

3. Базы данных периодических изданий:

3.1. База данных периодических изданий EastView : электронные журналы / ООО ИВИС. - Москва, [2022]. – URL: https://dlib.eastview.com/browse/udb/12. – Режим доступа : для авториз. пользователей. – Текст : электронный.

3.2. eLIBRARY.RU: научная электронная библиотека : сайт / ООО Научная Электронная Библиотека. – Москва, [2022]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

3.3. Электронная библиотека «Издательского дома «Гребенников» (Grebinnikon) : электронная библиотека / ООО ИД Гребенников. – Москва, [2022]. – URL: https://id2.action-media.ru/Personal/Products. – Режим доступа : для авториз. пользователей. – Текст : электронный.

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2022]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. SMART Imagebase : научно-информационная база данных EBSCO // EBSCOhost : [портал]. – URL: https://ebsco.smartimagebase.com/?TOKEN=EBSCO-1a2ff8c55aa76d8229047223a7d6dc9c&custid=s6895741. – Режим доступа : для авториз. пользователей. – Изображение : электронные.

6. Федеральные информационно-образовательные порталы:

6.1. Единое окно доступа к образовательным ресурсам : федеральный портал . – URL: http://window.edu.ru/ . – Текст : электронный.

6.2. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

7. Образовательные ресурсы УлГУ:

7.1. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

СОГЛАСОВАНО:

зам нач УИТиТ	Ключкова ВВ		03.06.2022г.
Должность сотрудника УИТиТ	ФИО	подпись	дата

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Учебный корпус по адресу: ул. Пушкинская, 4а. Объект доступен для маломобильных групп населения. Перед корпусом установлены дорожные знаки «Парковка для инвалидов». На стене у входа в здание установлены кнопка вызова дежурного и информационное устройство с тактильной идентификацией для помощи перемещения людей с ограниченными возможностями «Кнопка вызова персонала». На центральном крыльце корпуса установлены наклонные подъемные платформы. В корпусе имеется лифт и информационные устройства с тактильной идентификацией для помощи перемещения людей с ограниченными возможностями «Лифт для инвалидов» и «Направление движения». Ширина дверных проемов в тамбуре и вестибюле составляет 1200 мм. Дверные проемы не имеют порогов и перепадов высот пола. Имеется доступная ширина пути движения в коридорах. На первом этаже предусмотрена универсальная санитарно-гигиеническая кабина, доступная для всех маломобильных групп населения.

Здание института экономики и бизнеса (средство обучения). г.Ульяновск, ул. Федерации, д.№29. 1620,3. Объект не доступен для маломобильных групп населения. На стене у входа в здание установлены кнопка вызова дежурного и информационное устройство с тактильной идентификацией для помощи перемещения людей с ограниченными возможностями «Кнопка вызова персонала».

– Аудитории для проведения лекционных и семинарских занятий, оснащенные проектором, ноутбуком, аудиооборудованием для просмотра видео (6 аудитория, актовый зал, 703, 709 и др. аудитории в корпусах по ул.Федерации, 29 и по ул. Пушкинская, 4а).

– Аудитории, оборудованные интерактивными досками (603, 611).

– Аудитории для проведения тестирования и самостоятельной работы студентов с выходом в интернет, комп.класс №1к (корпус по ул. Федерации, 29).

– Читальный зал (803 аудитория) с компьютеризированными рабочими местами для работы с электронными библиотечными системами, каталогом и т.д.

13.СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

Обучение по ОПОП ВО обучающихся с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся. Образование обучающихся с огра-

ниченными возможностями здоровья может быть организовано как совместно с другими обучающимися, так и отдельно. В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации».

Разработчик _____ доцент Сковиков А.Г.

подпись должность ФИО