


Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		



**УТВЕРЖДЕНО**  
 решением ученого совета ИЭиБ  
 от 20 июня 2024 г., протокол № 10 / 271  
 Председатель \_\_\_\_\_ И.Б.Романова  
 « 20 » июня 2024 г.

### РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	<b>Информационная безопасность</b>
Факультет	экономики
Кафедра	цифровой экономики
Курс	5 / 6

Специальность: 38.05.01 «Экономическая безопасность»  
 Специализация: «Экономическая безопасность предпринимательской деятельности»  
 Форма обучения: очная, заочная

Дата введения в учебный процесс УлГУ: « 01 » сентября 2024 г.



Программа актуализирована на заседании кафедры: протокол № \_\_ от \_\_\_\_\_ 20\_\_ 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 Анатолий Геннадьевич	ЦЭ	доцент, к.т.н, доцент

СОГЛАСОВАНО	СОГЛАСОВАНО
Заведующий кафедрой ЦЭ	Заведующий выпускающей кафедрой ЭиП
 / Лутошкин И.В. / «20» июня 2024 г.	 / Рожкова Е.В. / «20» июня 2024 г.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Информационная безопасность» 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;
- изучение проблем защиты информации, стоящих перед современной вычислительной техникой;
- 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

Дисциплина «Информационная безопасность» принадлежит обязательной части Блока Б1 «Дисциплины (модули)» основной профессиональной образовательной программы (ОПОП). Она является одной из основополагающих дисциплин в системе подготовки специалиста по направлению 38.05.01 «Экономическая безопасность». Вместе с другими курсами, посвященными трендам трансформации 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

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

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.О.38.

Дисциплина читается в 9-ом семестре студентам 5-го курса очной формы обучения и базируется на отдельных компонентах компетенций, сформированных у обучающихся в ходе изучения предшествующих учебных дисциплин учебного плана. Студенты заочной формы обучения изучают дисциплину на 6-ом курсе.

**Пререквизиты.** Дисциплина рассчитана на студентов, 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. Помимо этого, для успешного освоения данного курса студент должен иметь навык самостоятельной работы с различными источниками информации (интернет, печатные издания), умением обобщать информацию, полученную из разных источников, умением представлять результаты своих исследований. Кроме этого, изучение курса базируется на компетенциях, сформированных у обучающихся в процессе изучения дисциплин:

- очная форма обучения –
  - Математика (ОПК-2; ОПК-3; ОПК-6).
- заочная форма обучения –
  - Математика (ОПК-2; ОПК-3; ОПК-6).

**Постреквизиты.** Знания, навыки и умения, приобретенные в результате прохождения курса, будут востребованы при прохождении преддипломной практики, защите выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

### 3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОПОП

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- *Способен использовать современные информационные технологии и программные средства при решении профессиональных задач. (ОПК-6).*

–

Код компетенции	Формулировка компетенции	Код индикатора компетенции	Индикаторы достижения компетенции
ОПК-6	Способен использовать современные информационные технологии и программные средства при решении профессиональных задач	ИД-1пк1	<b>знать:</b> ИД-1 опкб - типовые цифровые технологии проведения анализа и разработки управленческих решений в сфере информационной безопасности организации; ИД-1.1 опкб - основные понятия информационной безопасности. ИД-1.2 опкб - основные угрозы и способы классификации угроз информационной безопасности
		ИД-2пк1	<b>уметь:</b> ИД-2 опкб - использовать безопасные информационные технологии в своей профессиональной деятельности; ИД-2.1 опкб - формировать информационную базу для разработки решений в сфере информационной безопасности организации. ИД-2.2 опкб - анализировать информационную безопасность многопользовательских систем
		ИД-3пк1	<b>владеть:</b> ИД-3 опкб - навыками обеспечения безопасной работы на компьютере; ИД-3.1 опкб - навыками безопасного поиска информации в глобальной информационной сети Интернет.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

		ИД-3.2 опкб - методами обеспечения информационной безопасности жизненного цикла информационного контента предприятия и Интернет-ресурсов.
--	--	--

#### 4. ОБЪЕМ ДИСЦИПЛИНЫ


4.1. Объем дисциплины в зачетных единицах (всего) – 3 ЗЕТ.

4.2. Объем дисциплины по видам учебной работы (в часах): 108.

Вид учебной работы	Количество часов (форма обучения – очная)	
	Всего по плану	в т.ч. по семестрам <b>9</b>
Контактная работа обучающихся с преподавателем в соответствии с УП	54	54
Аудиторные занятия:		
• лекции	18	18
• семинары и практические занятия	36	36
• лабораторные работы, практикумы		
Самостоятельная работа	54	54
Форма текущего контроля знаний и контроля самостоятельной работы:	тестирование; реферат	тестирование; реферат
Курсовая работа	-	-
Виды промежуточной аттестации	Зачет	Зачет
<b>Всего часов по дисциплине</b>	<b>108</b>	<b>108</b>

Вид учебной работы	Количество часов (форма обучения – заочная)	
	Всего по плану	в т.ч. по семестрам <b>11</b>
Контактная работа обучающихся с преподавателем в соответствии с УП	12/12*	12/12*
Аудиторные занятия:		
• лекции	4/4*	4/4*
• семинары и практические занятия	8/8*	8/8*
• лабораторные работы, практикумы		
Самостоятельная работа	92	92
Форма текущего контроля знаний и контроля самостоятельной работы:	тестирование; реферат	тестирование; реферат
Курсовая работа	-	-
Виды промежуточной аттестации	Зачет (4/4*)	Зачет (4/4*)
<b>Всего часов по дисциплине</b>	<b>108</b>	<b>108</b>

\* В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, указанные часы работы ППС с обучающимися проводятся в дистанционном формате с применением электронного обучения

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

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

Форма обучения – очная

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			
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>	<i>8</i>
1. Введение в информационную безопасность.	22	4	8			10	тестирование, защита реферата
2. Обеспечение информационной безопасности на законодательном уровне.	12	2				10	тестирование, защита реферата
3. Обеспечение информационной безопасности на административном уровне.	14	4				10	тестирование, защита реферата
4. Обеспечение информационной безопасности на процедурном уровне.	14	4				10	тестирование, защита реферата
5. Программно-технические средства обеспечения информационной безопасности.	46	4	28			14	тестирование, защита реферата
<i>Зачет по дисциплине</i>	-	-	-	-	-	-	-
<b>ИТОГО:</b>	<b>108</b>	<b>18</b>	<b>36</b>			<b>54</b>	-

Форма обучения – заочная

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			
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>	<i>8</i>
1. Введение в информационную безопасность.	25	1	4			20	тестирование, защита реферата
2. Обеспечение информационной безопасности на законодательном	21	1				20	тестирование, защита реферата



Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

уровне.							
3. Обеспечение информационной безопасности на административном уровне.	21	1				20	тестирование, защита реферата
4. Обеспечение информационной безопасности на процедурном уровне.	20					20	тестирование, защита реферата
5. Программно-технические средства обеспечения информационной безопасности.	17	1	4			12	тестирование, защита реферата
<i>Зачет по дисциплине</i>	4	-	-	-		-	-
<b>ИТОГО:</b>	<b>108</b>	<b>4</b>	<b>8</b>			<b>92</b>	<b>-</b>

## 5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

### Тема 1. Введение в информационную безопасность.

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. 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. Ис-

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

пользование 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 2. Обеспечение информационной безопасности на законодательном уровне.**

Уровни защиты информации. Ключевые понятия информационной безопасности – политика безопасности и программа безопасности. Структура соответствующих документов, меры по их разработке и сопровождению. Этапы жизненного цикла информационных систем и меры безопасности. Что такое законодательный уровень информационной безопасности и почему он важен. Обзор российского законодательства в области защиты информации. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности. Обзор зарубежного законодательства в области информационной безопасности. О текущем состоянии российского законодательства в области информационной безопасности. Понятие стандарта. Классификация стандартов в области информационной безопасности. «Оранжевая книга», ее структура и группы классов защищенности. Руководящие документы Гостехкомиссии России. Тезисы из руководящего документа «Средства вычислительной техники. Защита от НСД к информации». Показатели защищенности от НСД к информации». Тезисы из руководящего документа «Автоматизированные системы. Защита от НСД информации». Основные идеи документа «Общие критерии» ISO/IEC 15408-1999. Понятие профиля защиты (ПЗ) и Задания по безопасности (ЗБ). Основные положения международного стандарта ISO/IEC 17799:2005. Основные положения международного стандарта ISO/IEC 27001:2005. Основные положения британского стандарта BS 7799-3:2006.

## **Тема 3. Обеспечение информационной безопасности на административном уровне.**

Политика безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом систем. Методика, позволяющая сопоставить возможные потери от нарушений ИБ со стоимостью защитных средств. Оценка рисков: выбор анализируемых объектов и уровня детализации их рассмотрения; выбор методологии оценки рисков; идентификация активов; анализ угроз и их последствий, выявление уязвимых мест в защите; оценка рисков; выбор защитных мер; реализация и проверка выбранных мер; оценка остаточного риска.

## **Тема 4. Обеспечение информационной безопасности на процедурном уровне.**

Основные классы мер процедурного уровня: управление персоналом; физическая защита; поддержание работоспособности; реагирование на нарушения режима безопасности; планирование восстановительных работ.

## **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. Идентифика-



Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

ция/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 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 Proxu 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 кото-

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

рых 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

№ п/п	№ темы	Тема семинара	Кол-во часов
1	1	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.	8
2	5	Управление доступом. Матрица доступа. Произвольное (или дискреционное) управление доступом. Принудительное (мандатное) управление доступом. Списки управления доступом. Основы Active Directory Domain Services. Основы работы с групповыми политиками.	4
3	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 Гамала. Алгоритм цифровой подписи DSA.	8
4	5	Применение аудита в ОС семейства Windows для отслеживания деятельности пользователей. Настройка политики аудита. Аудит в Windows Server 2008/2012.	4
5	5	Механизмы защиты, реализуемые межсетевым экраном (МЭ):	8

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

		<p>фильтрация сетевого трафика; шифрование (создание VPN); трансляция адресов; аутентификация (дополнительная); противодействие некоторым сетевым атакам; управление списками доступа на маршрутизаторах.</p> <p>Типы межсетевых экранов. Пакетные фильтры. Шлюзы уровня соединения. Stateful Inspection firewall. Host-based firewall. Примеры правил.</p> <p>Персональные firewall и персональные устройства firewall. Шлюзы прикладного уровня. Прокси-сервер прикладного уровня. Выделенные прокси-серверы. Примеры правил. Трансляция сетевых адресов (NAT).</p> <p>Концепция построения защищённых виртуальных частных сетей VPN. Функции и компоненты сети VPN. VPN решения для построения защищённых корпоративных сетей.</p>	
6	5	Троянские программы. Сетевые черви. Антивирусное ПО. Обнаружение компьютерных вирусов. Комплексная система защиты информации.	4
		<b>Итого:</b>	<b>36</b>

## ТЕМА 1. ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ЗАНЯТИЕ 1

### Типовые удаленные атаки

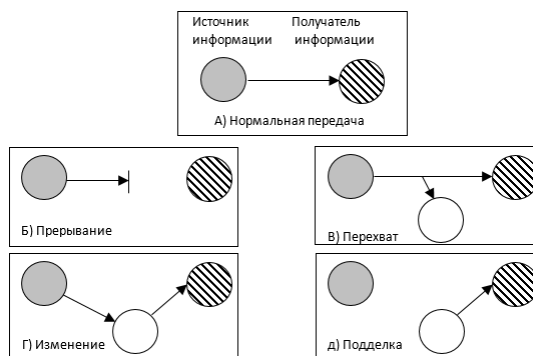
Форма проведения – семинар, дискуссия.

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

#### 1. Категории информации.



#### 2. Удаленные атаки на распределенные вычислительные системы.



Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

3. Характеристика и механизмы реализации типовых удаленных атак.
4. Понятие типовой удаленной атаки.

### ЗАНЯТИЯ 2, 3, 4

#### Примеры типовых удаленных атак

Форма проведения – семинар, дискуссия.

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

1. Анализ сетевого трафика.
2. Подмена доверенного объекта или субъекта РВС.
3. Ложный объект РВС.
4. Внедрение в РВС ложного объекта путем навязывания ложного маршрута.
5. Внедрение в РВС ложного объекта путем использования недостатков алгоритмов удаленного поиска.
6. Использование ложного объекта для организации удаленной атаки на РВС.
7. Селекция потока информации и сохранение ее на ложном объекте РВС.
8. Модификация информации.
9. Подмена информации.
10. Отказ в обслуживании.

## ТЕМА 5. ПРОГРАММНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

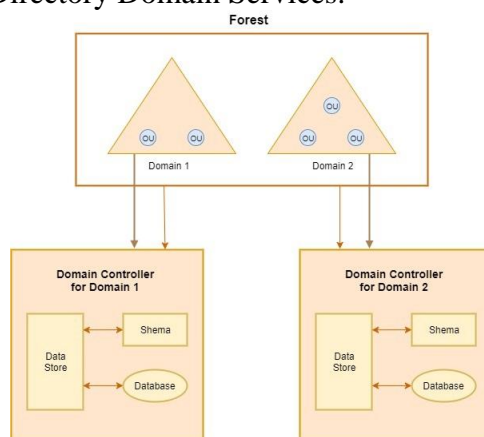
### ЗАНЯТИЯ 5, 6

#### Сервис информационной безопасности - Управление доступом

Форма проведения – семинар, дискуссия.

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

1. Управление доступом.
2. Матрица доступа.
3. Произвольное (или дискреционное) управление доступом.
4. Принудительное (мандатное) управление доступом.
5. Списки управления доступом.
6. Ролевое управление доступом.
7. Основы Active Directory Domain Services.



8. Основы работы с групповыми политиками.

### ЗАНЯТИЕ 7, 8

#### Примеры основных криптографических алгоритмов

Форма проведения – семинар, дискуссия, деловая игра.

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

1. Симметричные и асимметричные криптосистемы.
2. Алгоритмы замены и перестановки.
3. Алгоритм шифрования DES и его модификации.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

4. Генерация и хранение ключей.
5. Распределение ключей.
6. Управление ключами в системах с открытым ключом.
7. Алгоритм Диффи-Хелмана.

### **ЗАНЯТИЕ 9, 10**

#### **Примеры основных криптографических алгоритмов**

Форма проведения – семинар, дискуссия.

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

1. Основные свойства цифровой подписи.
2. Алгоритм цифровой подписи RSA.
3. Алгоритм цифровой подписи Эль Гамала.
4. Алгоритм цифровой подписи DSA.

### **ЗАНЯТИЯ 11, 12**

#### **Сервис информационной безопасности - Аудит**

Форма проведения – семинар, дискуссия.

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

1. Применение аудита в ОС семейства Windows для отслеживания деятельности пользователей.
2. Настройка политики аудита.
3. Аудит в Windows Server 2008/2012.

### **ЗАНЯТИЯ 13, 14**

#### **Сервис информационной безопасности - Межсетевые экраны**

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.

### **ЗАНЯТИЯ 15, 16**

#### **Категории межсетевых экранов**

Форма проведения – семинар, дискуссия.

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


1. Типы межсетевых экранов.
2. Пакетные фильтры.
3. Шлюзы уровня соединения.
4. Stateful Inspection firewall.
5. Host-based firewall.
6. Примеры правил.
7. Персональные firewall и персональные устройства firewall.
8. Шлюзы прикладного уровня.
9. Прокси-сервер прикладного уровня.
10. Выделенные прокси-серверы.
11. Примеры правил.
12. Трансляция сетевых адресов (NAT).
13. Функции и компоненты сети VPN.
14. VPN решения для построения защищённых корпоративных сетей.

### **ЗАНЯТИЯ 17, 18**

#### **Вирусы**

Форма проведения – семинар, дискуссия.

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

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

1. Категории вирусы.
2. Классические вирусы.
3. Макровирусы.
4. Троянские программы.
5. Сетевые черви.
6. Антивирусное ПО.
7. Обнаружение компьютерных вирусов.
8. Комплексная система защиты информации.

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. Преподаватель 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**

Реферат это одна из форм текущего контроля знаний и контроля самостоятельной работы. Реферат – это самостоятельная исследовательская работа, в которой автор рас-



Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

крывает 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	Виды защищаемой информации.
6	Демаскирующие признаки объектов защиты.
7	Классификация источников и носителей информации.
8	Мероприятия по управлению доступом к информации.
9	Функциональные источники сигналов. Опасный сигнал.
10	Основные средства и системы, содержащие потенциальные источники опасных сигналов.
11	Вспомогательные средства и системы, содержащие потенциальные источники опасных сигналов.
12	Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей.
13	Виды угроз безопасности информации.
14	Основные принципы добывания информации.
15	Процедура идентификации, как основа процесса обнаружения недоверенного объекта.
16	Методы синтеза информации.
17	Методы несанкционированного доступа к информации.
18	Основными способами 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.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

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	Общая теория криптографии.
61	Различные методы шифрования.
62	Отечественные и зарубежные стандарты шифрования.
63	Общая характеристика и классификация компьютерных вирусов.
64	Механизм заражения файловыми и загрузочными вирусами. Особенности макровирусов.

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

65	Средства, используемые для обнаружения компьютерных вирусов.
66	Профилактика заражения компьютерными вирусами.
67	Антивирусные средства для лечения и удаления компьютерных вирусов. Программы-полифаги. Эвристические анализаторы.

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 зачитан 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».

Курсовые и контрольные работы не предусмотрены УП.

## 9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ (ЗАЧЕТУ)

№	Формулировка вопроса
1	Понятие информационной безопасности
2	Основные составляющие информационной безопасности
3	Основные определения и критерии классификации угроз
4	Классификация типовых удаленных атак
5	Основные понятия программно-технического уровня информационной безопасности
6	Сервис безопасности идентификация и аутентификация
7	Сервис безопасности управление доступом
8	Сервис безопасности протоколирование и аудит
9	Сервис безопасности шифрование
10	Сервис безопасности контроль целостности
11	Сервис безопасности экранирование
12	Сервис безопасности анализ защищенности
13	Сервис безопасности обеспечение отказоустойчивости
14	Сервис безопасности обеспечение безопасного восстановления

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

15	Сервис безопасности туннелирование
16	Сервис безопасности управление
17	Классификация вирусов
18	Средства антивирусной защиты
19	Типовая удаленная атака «Анализ сетевого трафика»
20	Типовая удаленная атака «Подмена доверенного объекта или субъекта распределенной вычислительной системы»
21	Типовая удаленная атака «Внедрение в распределенную вычислительную систему ложного объекта путем навязывания ложного маршрута»
22	Типовая удаленная атака «Отказ в обслуживании»
23	Ложный ARP-сервер в сети Internet
24	Ложный DNS-сервер в сети Internet
25	Навязывание хосту ложного маршрута с использованием протокола ICMP с целью создания в сети Internet ложного маршрутизатора
26	Подмена одного из субъектов TCP-соединения в сети Internet
27	Причины успеха удаленных атак на распределенные вычислительные системы
28	Криптография
29	Какие цели преследует криптография? Перечислите основные алгоритмы криптографических преобразований
30	Перечислите основные методы криптографической защиты информации в компьютерных системах и сетях
31	Как классифицируются средства криптографической защиты информации?
32	Перечислите основные схемы идентификации пользователя
33	Преимущества и недостатки асимметричных криптосистем. С какой целью в асимметричных криптосистемах используются два ключа?
34	Как обеспечивается криптостойкость асимметричных криптосистем?
35	Каково основное назначение хэш-функций? Каковы основные принципы формирования хэш-функций? Какими свойствами должна обладать хэш-функция, используемая в процессе аутентификации?
36	Где и с какой целью используется электронная цифровая подпись? Перечислите основные этапы формирования электронной цифровой подписи. Какими свойствами должна обладать электронная цифровая подпись? Перечислите основные алгоритмы электронной цифровой подписи и укажите на их принципиальные отличия
37	Достоинства биометрических способов идентификации и аутентификации по сравнению с традиционными
38	Перечислите функции и компоненты сети VPN
39	Классифицируйте VPN по способу технической реализации и архитектуре технического решения
40	Каковы способы защиты информации при межсетевом взаимодействии?
41	Стандарты в информационной безопасности. Понятие стандарта.
42	Классификация стандартов в области информационной безопасности. «Оранжевая книга», ее структура и группы классов защищенности.
43	Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»
44	Административный уровень информационной безопасности. Основные понятия. Политика безопасности. Программа безопасности
45	Сервисы безопасности
46	Классификация удаленных атак на распределенные вычислительные системы

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		


47	Понятие типовой удаленной атаки
48	Классические вирусы
49	Троянские программы
50	Сетевые черви

## 10. САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ

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 – очная.

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1. Введение в информационную безопасность.	– Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины; – Подготовка к тестированию; – Подготовка к сдаче экзамена	10	тестирование, реферат, экзамен
2. Обеспечение информационной безопасности на законодательном уровне.	– Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины; – Подготовка к тестированию; – Подготовка к сдаче экзамена	6	тестирование, реферат, экзамен
3. Обеспечение информационной безопасности на административном уровне.	– Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины; – Подготовка к тестированию; – Подготовка к сдаче экзамена	6	тестирование, реферат, экзамен
4. Обеспечение информационной безопасности на процедурном уровне.	– Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины; – Подготовка к тестированию; – Подготовка к сдаче экзамена	4	тестирование, реферат, экзамен
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	10	тестирование, реферат, экзамен

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

Форма обучения – заочная.

Название разделов и тем	Вид самостоятельной работы	Объем в часах	Форма контроля
1. Введение в информационную безопасность.	– Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины; – Подготовка к тестированию; – Подготовка к сдаче экзамена	20	тестирование, реферат, экзамен
2. Обеспечение информационной безопасности на законодательном уровне.	– Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины; – Подготовка к тестированию; – Подготовка к сдаче экзамена	20	тестирование, реферат, экзамен
3. Обеспечение информационной безопасности на административном уровне.	– Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины; – Подготовка к тестированию; – Подготовка к сдаче экзамена	20	тестирование, реферат, экзамен
4. Обеспечение информационной безопасности на процедурном уровне.	– Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины; – Подготовка к тестированию; – Подготовка к сдаче экзамена	20	тестирование, реферат, экзамен
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	12	тестирование, реферат, экзамен

#### 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:



Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

- 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 выполнение. 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 не-

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

посредственную 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 приобретает 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 приближе-

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

ние 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) Список рекомендуемой литературы

#### Основная:

Зенков Андрей Вячеславович. Информационная безопасность и защита информации : Учебное пособие для вузов / А.В. Зенков ; Зенков А. В. - Москва : Юрайт, 2022. - 104 с. - (Высшее образование). - URL: <https://urait.ru/bcode/497002>

Суворова Галина Михайловна. Информационная безопасность : Учебное пособие для вузов / Г.М. Суворова ; Суворова Г. М. - Москва : Юрайт, 2022. - 253 с. - (Высшее образование). - URL: <https://urait.ru/bcode/496741>

#### Дополнительная:

Корабельников Сергей Маркович. Преступления в сфере информационной безопасности : Учебное пособие для вузов / С.М. Корабельников ; Корабельников С. М. - Москва : Юрайт, 2022. - 111 с. - (Высшее образование). - URL: <https://urait.ru/bcode/496492>

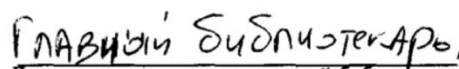
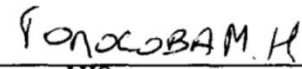

Внуков Андрей Анатольевич. Защита информации в банковских системах : Учебное пособие для вузов / А.А. Внуков ; Внуков А. А. - 2-е изд. ; испр. и доп. - Москва : Юрайт, 2022. - 246 с. - (Высшее образование). - URL: <https://urait.ru/bcode/490278>

Гродзенский, Я.С. Информационная безопасность : учебное пособие / Я. С. Гродзенский ; Гродзенский Я.С. - Москва : РГ-Пресс, 2020. - 144 с. - URL: <https://www.studentlibrary.ru/book/ISBN9785998808456.html>

#### Учебно-методическая:

1. Сковиков, А. Г. Методические указания для самостоятельной работы студентов по дисциплине «Информационная безопасность» для студентов специальности 38.05.01 «Экономическая безопасность» (специалитет) / А. Г. Сковиков ; УлГУ, ИЭиБ, Каф. цифровой экономики. - Электрон. текстовые дан. (1 файл : 431КБ). - Ульяновск : УлГУ, 2018. - Загл. с экрана. - Неопубликованный ресурс. - Режим доступа: ЭБС УлГУ. - Текст : электронный. - URL: <http://lib.ulsu.ru/MegaPro/Download/MObject/2688>

Согласовано:




03.06.2024 г.  
 Должность сотрудника научной библиотеки      ФИО      подпись      дата

Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

**б) Программное обеспечение –**  
Операционная система "Альт образование"  
Офисный пакет "Мой офис"

**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, [2024]. – 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, [2024]. - 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, [2024]. – 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, [2024]. – URL: <https://e.lanbook.com>. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. ЭБС Znanium.com : электронно-библиотечная система : сайт / ООО «Знаниум». - Москва, [2024]. - 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, [2024].

**3. eLIBRARY.RU:** научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2024]. – URL: <http://elibrary.ru>. – Режим доступа : для авториз. пользователей. – Текст : электронный

**4. Федеральная государственная информационная система «Национальная электронная библиотека» :** электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2024]. – URL: <https://нэб.рф>. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

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

**6. 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.

Инженер ведущий



Щуренко Ю.В.

03.06.2024



Министерство науки и высшего образования РФ Ульяновский государственный университет	Форма	
Ф - Рабочая программа дисциплины		

## 12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Аудитории для проведения лекций, семинарских занятий, для выполнения лабораторных работ и практикумов, для проведения текущего контроля и промежуточной аттестации, курсового проектирования, групповых и индивидуальных консультаций.

Аудитории укомплектованы специализированной мебелью, учебной доской. Аудитории для проведения лекций оборудованы мультимедийным оборудованием для предоставления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде, электронно-библиотечной системе.

В том числе:

1. Аудитории для проведения лекционных и семинарских занятий, оснащенные проектором, ноутбуком (актовый зал, 703, 709, 509 и др. аудитории).
2. Аудитории для проведения практических и лабораторных занятий (комп. классы – аудитории 1К, 49, 508, 711, 605, 407). Всего 63 рабочих места.
3. Аудитории, оборудованные интерактивными досками (603, 611, 502).
4. Аудитории для проведения тестирования и самостоятельной работы студентов с выходом в интернет, комп.класс №806 (корпус по ул. Пушкинская, 4а), 1 сервер и 16 рабочих мест.
5. Читальный зал (аудитория 803) 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.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик



доцент кафедры А.Г. Сквиков