МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кемеровский государственный университет»
Кузбасский гуманитарно-педагогический институт

(Наименование филиала, где реализуется данная дисциплина)

Факультет психологии и педагогики

УТВЕРЖДАЮ

Декан ФПП

____________ Л. Я. Лозован

«23» марта 2023 г.

Рабочая программа дисциплины

Б1.В.ДВ.05.02 Информационная безопасность в служебной деятельности

Код, название дисциплины

Специальность
37.05.02 Психология служебной деятельности

Специализация
Морально-психологическое обеспечение служебной деятельности

Программа специалитета

Квалификация выпускника
Психолог

Форма обучения
Очная, очно-заочная

Год набора 2019

Новокузнецк, 2023

Лист внесения изменений

В РПД Б1.В.ДВ.05.02 Информационная безопасность в служебной деятельности

(код по учебному плану, название дисциплины)

Сведения об утверждении:
утверждена Ученым советом факультета психологии и педагогики
(протокол Ученого совета факультета № 9 от 23.03.2023 г.)

для ОПОП 2019 года набора на 2023 / 2024 учебный год
по специальности 37.05.02 Психология служебной деятельности

специализация / «Морально-психологическое обеспечение служебной деятельности»

Одобрена на заседании методической комиссии факультета психологии и педагогики
протокол методической комиссии факультета № 6 от 22.03.2023 г.)

Одобрена на заседании обеспечивающей кафедры психологии и общей педагогики

протокол № 7 от 07.03.2023 г. Алонцева А. И. / _____
(Ф. И.О. зав. кафедрой)

Оглавление

1. Цель дисциплины

В результате освоения данной дисциплины у обучающегося должны быть сформированы компетенции основной профессиональной образовательной программы специалитета (далее - ОПОП): ПК-14способность разрабатывать и реализовывать программы, направленные на предупреждение нарушений и отклонений в социальном и личностном статусе, психическом развитии сотрудников, военнослужащих и иных лиц, рисков асоциального поведения, профессиональных рисков, профессиональной деформации.

Содержание компетенций как планируемых результатов обучения по дисциплине см. таблицы 1 и 2.

1.1 Формируемые компетенции

Таблица 1 - Формируемые дисциплиной компетенции

Наименование вида компетенции	Код и название компетенции
профессиональная	ПК-14 способность разрабатывать и реализовывать программы, направленные на предупреждение нарушений и отклонений в социальном и личностном статусе, психическом развитии сотрудников, военнослужащих и иных лиц, рисков асоциального поведения, профессиональных рисков, профессиональной деформации

1.2 Дисциплины и практики, участвующие в формировании компетенций

Таблица 2 – Дисциплины и практики, формирующие компетенции данной дисциплины

Код и название компетенции	Дисциплины и практики, формирующие компетенцию ОПОП
ПК-14 способность разрабатывать и реализовывать программы, направленные на предупреждение нарушений и отклонений в социальном и личностном статусе, психическом развитии сотрудников, военнослужащих и иных лиц, рисков асоциального поведения, профессиональных рисков, профессиональной деформации	Б1.Б.13 Психология конфликта Б1.Б.34 Пенитенциарная психология Б1.В.01 Методы профилактики профессиональной деф Б1.В.08 Тренинговые технологии в работе психолога с Б1.В.08.02 Тренинг личностного роста Б1.В.08.04 Технология группового тренинга Б1.В.14 Психология агрессивного поведения субъекто Б1.В.ДВ,02.01 Психология девиантного и аддиктивно Б1.В.ДВ.02.02 Базовые теории и методы психотерапи Б1.В.ДВ.05.01 Психология безопасности Б1.В.ДВ.05.02 Информационная безопасность в служе Б2.Б.02 (П) Практика по получению профессиональны Б2.Б.03(Пд) Преддипломная Б3.Б.02(Д) Выпускная квалификационная работа

1.3 Знания, умения, навыки (ЗУВ) по дисциплине

Таблица 3 – Знания, умения, навыки, формируемые дисциплиной

Код и название компетенции	Знания, умения, навыки (ЗУВ), формируемые дисциплиной
ПК-14 способность разрабатывать и реализовывать программы, направленные на предупреждение нарушений и отклонений в социальном и личностном статусе, психическом развитии сотрудников, военнослужащих и иных лиц, рисков асоциального поведения, профессиональных рисков, профессиональной деформации	**Знать:** – риски асоциального поведения и признаки профессиональной деформации сотрудников, военнослужащих и иных лиц. **Уметь:** – разрабатывать программы, направленные на предупреждение нарушений и отклонений в социальном и личностном статусе, психическом развитии сотрудников, военнослужащих и иных лиц. **Владеть:** – навыками разработки и реализации программ, направленных на предупреждение нарушений и отклонений в социальном и личностном статусе, профессиональной деформации.

2. Объём и трудоёмкость дисциплины по видам учебных занятий. Формы промежуточной аттестации

Таблица 4 – Объем и трудоемкость дисциплины по видам учебных занятий

Общая трудоемкость и виды учебной работы по дисциплине, проводимые в разных формах	Объём часов по формам обучения	
	ОФО	ОЗФО
1 Общая трудоемкость дисциплины	180	180
2 Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	64	22
Аудиторная работа (всего):	64	22
в том числе:		
лекции	30	10
практические занятия, семинары	34	12
в интерактивной форме		4
3 Самостоятельная работа обучающихся (всего)	80	122
4 Промежуточная аттестация обучающегося	36 (экзамен 6 семестр)	36 (экзамен 9 семестр)

3. Учебно-тематический план и содержание дисциплины

3.1 Учебно-тематический план

Таблица 5 - Учебно-тематический план очной и очно-заочной формы обучения

№ п/п	Разделы дисциплины по занятиям	Общая трудоёмкость *(всего час.)*	Трудоемкость занятий (час.)						Формы текущего контроля и промежуточной аттестации успеваемости
			ОФО			ОЗФО			
			Аудиторн. занятия		СРС	Аудиторн. занятия		СРС	
			лекц.	практ.		лекц.	практ.		
1.	Информатизация общества и информационная безопасность	22	6	6	10	0	2	20	Тест
2.	Нормативно-правовое обеспечение информационной безопасности в Российской Федерации	24	6	4	14	2	2	22	Тест
3.	Организация противодействия компьютерной преступности	26	6	6	14	2	2	20	Тест
4.	Типовые решения по безопасности компьютерных сетей	24	4	6	14	2	2	20	Тест
5.	Организация противодействия вредоносным программам	24	4	6	14	2	2	20	Тест
6.	Криптография как метод обеспечения информационной безопасности	24	4	6	14	2	2	20	Тест
7.	**Экзамен**	**36**	0	0	0	0	0	0	
	Итого	**180**	**30**	**34**	**80**	**10**	**12**	**122**	

3.2. Содержание занятий по видам учебной работы

Таблица 6 – Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание занятий
1	**Информатизация общества и информационная безопасность**	
Содержание лекционного курса		
1.1.	Введение в предмет. Угрозы информационной безопасности	Введение в предмет. Цели и задачи изучения дисциплины. Особенности учебной работы по дисциплине.
1.2	Методологические основы безопасности.	Учебные планы, учебно-методические комплексы, рабочие программы, методические рекомендации и указания.
1.3	Основные принципы информационной безопасности.	Принцип законности и правовой обеспеченности. Принцип баланса интересов личности, общества и государства. Принцип интеграции с международными системами безопасности. Принцип экономической эффективности. Принцип комплексности, системности.

Темы практических / семинарских занятий		
1	Рассмотрение конфликтов в организациях	**Семинар** Конфликты, обусловленные требованиями режима Конфликты, обусловленные несоответствием ожиданий и реальности, конфликты «несбывшихся надежд» Конфликты «человек – система» Конфликты, обусловленные ограниченностью ресурсов Конфликты, обусловленные несоответствием целей сотрудников системы защиты информации и других работников и отделов Конфликты иерархии Конфликт «формальной и неформальной структур» (формальный руководитель и неформальный лидер), борьба за власть. **СРС:** подготовить темы докладов и рассказать о них.
2	Криминалистическая характеристика компьютерных преступлений в России	**Семинар** Криминалистическая характеристика компьютерных преступлений Обстановка совершения преступления Свойства личности субъекта преступления Предупреждение компьютерных преступлений Составьте «портрет» характерологических черт личности склонной к совершению информационного преступления
3	Проверка знаний	Перечислите виды конфликтов. Дайте характеристику компьютерным преступлениям. Укажите основные принципы информационной безопасности.
2	**Нормативно-правовое обеспечение информационной безопасности в Российской**	
Содержание лекционного курса		
2.1.	Правовой режим информации	Нормативно-правовые акты федерального законодательства в области информационной безопасности. Произведения, пользующиеся охраной.
2.2.	Органы, обеспечивающие информационную безопасность	Государственные органы РФ, контролирующие деятельность в области защиты информации.
2.3.	Организационно-правовые основы защиты информации в органах внутренних дел	Основные составляющие национальных интересов Российской Федерации в информационной сфере.
Темы практических / семинарских занятий		

1	Органы, обеспечивающие информационную безопасность. Организационно-правовые основы защиты информации в органах внутренних дел	**Семинар** Основные задачи и функции Совета Безопасности Расскажите о федеральной службе по техническому и экспортному контролю Чем занимается федеральная служба безопасности Российской Федерации? Для чего нужна межведомственная комиссия по защите государственной тайны? Какие существуют угрозы безопасности информации и средствам информатизации? Какие существуют угрозы негативных информационно-психологических воздействий?
2	Проверка знаний	Что следует понимать под «правовым режимом информации»? Назовите несколько наиболее важных законов, регламентирующих информационные отношения в обществе. Поясните разницу между собственником, владельцем и пользователем информации. Перечислите органы защиты государственной тайны. Какая информация, по закону, не может быть закрытой? Перечислите основные нормативные документы по защите информации. Укажите категории информации ограниченного доступа. Поясните смысл категории «коммерческая тайна».
3	**Организация противодействия компьютерной преступности**	
Содержание лекционного курса		
3.1	Угрозы информационной безопасности и методы их реализации	Основные методы реализации угроз информационной безопасности АС. Три основных видов угроз.Классификация возможных угроз информационной безопасности АС.
3.2.	Ответственность за компьютерные преступления	Неправомерный доступ к компьютерной информации (ст. 272). Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273). Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274).

3.3.	Факторы развития компьютерной преступности	Доступ к информационным ресурсам. Развитие мировых и национальных компьютерных сетей и новых технологий Переводом информационных ресурсов на электронные носители. Концентрация в информационных системах. Разработка и совершенствование информационных технологий.Способность разрабатывать и реализовывать программы, направленные на предупреждение нарушений и отклонений в социальном и личностном статусе, психическом развитии сотрудников, военнослужащих и иных лиц, рисков асоциального поведения, профессиональных рисков, профессиональной деформации с учетом развития в современном мире компьютерной
Темы практических / семинарских занятий		
1	Методика раскрытия и расследования компьютерных преступлений	**Семинар** Что такое несанкционированный (неправомерный) доступ к компьютерной информации? Какие существуют нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети? Типичные следственные ситуации первоначального этапа и следственные действия. Опишите особенности производства осмотров и обысков. Что такое поиск и изъятие информации и следов воздействия на нее в ЭВМ и ее устройствах. Использование специальных познаний и назначение экспертиз.
2	Проверка знаний	Каковы структурные особенности УК РФ в области компьютерной преступности? Перечислите базовые классификационные признаки угроз информационной безопасности в автоматизированных системах. Укажите основные причины утечки информации на объектах информатизации. Что понимается под *несанкционированным доступом* в информационную систему? Перечислите категории компьютерных преступников.

	Проверка знаний	Назовите виды компьютерной преступности. Укажите способы совершения компьютерных преступлений. Какое максимальное наказание и по какой статье может назначить суд за компьютерное преступление? Как следует опечатывать ПЭВМ так, чтобы исключить возможность работы с ними? Укажите типичные следственные ситуации при расследовании компьютерных преступлений.
4	**Типовые решения по безопасности компьютерных сетей**	
Содержание лекционного курса		
4.1	Модели безопасного подключения к Internet	Что такое Internet? Цель формирования политики безопасности для Internet.
4.2	Принципы функционирования межсетевых экранов	Межсетевой экран. Типы атак в сети.
Темы практических / семинарских занятий		
1	Модели безопасного подключения к Internet	Дискуссия на тему: «Защита в Internet или от Internet?». Задача студентов привести доводы за ту точку зрения, которую считают верной.
2	Принципы функционирования межсетевых экранов	**Семинар** Что такое протокол TCP/IP? Что включает в себя понятие сокет? В чем состоит фундаментальная проблема безопасности Internet? Какие существуют две базовые политики межсетевого экрана?
3	Коллоквиум	Проверка знаний за первые разделы.
5	**Организация противодействия вредоносным программам**	
Содержание лекционного курса		
5.1	Понятие о вредоносных программах	Понятие вредоносных программ. Виды вредоносных программ.
5.2	Технологии обнаружения и нейтрализации вредоносных программ	Поведенческое противодействие. Технологии блокировки работы антивирусных продуктов. Методики загрузки информации из Интернета.
Темы практических / семинарских занятий		

1	Понятие о вредоносных программах	**Семинар** Каким документом регламентирован термин «вредоносные программы» и что это такое? Какие виды вредоносных программ существуют и охарактеризуйте их? Чем отличаются компьютерные вирусы от троянских программ?
2	Технологии обнаружения и нейтрализации вредоносных программ	**Семинар** Что такое использование ловушек для антируткитов? Что такое атаки на GUI? Что означает деструктивные вредоносные программы?
3	Проверка знаний по теме	**Семинар** Перечислите средства нейтрализации вирусов (вредоносных программ). Какие потери (затраты) и на что именно несут организации в связи с существованием явления «вредоносная программа»? Как вы думаете, что такое потери репутации и как они могут быть связаны с вредоносными программами? Укажите способы тиражирования антивирусного обеспечения.
6	**Криптография как метод обеспечения информационной безопасности**	
Содержание лекционного курса		
6.1	Основные понятия и элементы криптографии	Понятие «криптография». Возможные проблемы при обмене сообщениями.
6.2	Симметричные и асимметричные криптосистемы	Понятие «симметричные криптосистемы». Понятие «асимметричные криптосистемы». Их отличие друг от друга.
Темы практических / семинарских занятий		
1	Понятие цифровой подписи и цифрового сертификата	**Семинар** Что такое цифровая подпись? Расскажите об областях, в которых применяется цифровая подпись. Что нужно для обмена юридически значимыми электронными документами? Расскажите о юридической силе документа с электронной подписью. Какое существует нормативно-правовое поле использования электронной подписи.

2	Криптосистема	**Семинар** Что понимается под термином управление криптографическими ключами? Какова основная цель и основные задачи управления ключами? В чем, на ваш взгляд, отличие жизненного цикла секретных и открытых криптографических ключей? Изложите в общих чертах существо сертификации открытых ключей. Каким образом распространяются открытые ключи в криптосистемах?
3	Коллоквиум	Проверка знаний по последним разделам.

4 Порядок оценивания успеваемости и сформированности компетенций обучающегося в текущей и промежуточной аттестации

Для положительной оценки по результатам освоения дисциплины обучающемуся необходимо выполнить все установленные виды учебной работы. Оценка результатов работы обучающегося в баллах (по видам) приведена в нижеследующей таблице.

Таблица - Шкала и показатели оценивания результатов учебной работы обучающихся по видам в балльно-рейтинговой системе (БРС)

Учебная работа (виды)	Сумма баллов	Виды и результаты учебной работы	Оценка в аттестации (шкала и показатели оценивания)	Баллы
Текущая учебная работа ОФО				
ОФО Текущая учебная работа в семестре (посещение занятий по расписанию и выполнение заданий)	60 (100% / баллов приведенной шкалы)	Конспекты тем: 15 тем (рукописные)	**2 балла** - раскрытие темы на 51-65% **3 балла** раскрытие темы на 66 - 85% **4 балла** раскрытие темы на 86 - 100%	16-16
		Практические занятия (17 занятий)	**2 балла** - посещение 1 практического занятия и выполнение работы на 51-65% **4 балла** – посещение 1 занятия и существенный вклад на занятии в работу группы, самостоятельность и выполнение работы на 66 -100%	18-48
		Итоговый тест	**17 баллов** (51 - 65% правильных ответов) **18 баллов** (66 - 85% правильных ответов) **20 баллов** (86 - 100% правильных ответов)	17- 36
			Итого по текущей работе в семестре	51 - 100
Текущая учебная работа ОЗФО				
ОЗФО Текущая учебная работа в семестре (выполнение самостоятельных конспектов, теста)	60 (100% / баллов приведенной шкалы)	Конспекты тем: 5темы (рукописные).	**2 балла** - раскрытие темы на 51-65% **3 балла** раскрытие темы на 66 - 85% **4 балла**раскрытие темы на 86 - 100%	8 - 16
		Практические занятия (12 занятий).	**4 баллов** - посещение 1 практического занятия и выполнение работы на 51-65% **8 баллов** – посещение 1 занятия и существенный вклад на занятии в работу группы, самостоятельность и выполнение работы на 66 -100%	24-48
		Итоговый тест	**19 баллов** (51 - 65% правильных ответов) **28 баллов** (66 - 85% правильных ответов) **36 баллов** (86 - 100% правильных ответов)	19-36
			Итого по текущей работе в семестре	**51 - 100**
Промежуточная аттестация				
Промежуточная аттестация	**20** (100%	Вопрос	**10 баллов** (пороговое значение) **20 баллов** (максимальное значение)	10-20

(зачет)	/баллов приведенной шкалы)	Решение практико-ориентированного задания	**10 баллов** (пороговое значение) **20 баллов** (максимальное значение)	10-20
			Итого по промежуточной аттестации (зачет)	20-40
Суммарная оценка по дисциплине: Сумма баллов текущей и промежуточной аттестации				51 – 100 б.

В промежуточной аттестации оценка выставляется в ведомость в 100-балльной шкале и в буквенном эквиваленте.

Таблица – Соотнесение 100-балльной шкалы и буквенного эквивалента оценки

Сумма набранных баллов	Уровни освоения дисциплины и компетенций	*Экзамен*		*Зачет*
		Оценка	*Буквенный эквивалент*	*Буквенный эквивалент*
86 - 100	Продвинутый	5	отлично	Зачтено
66 - 85	Повышенный	4	хорошо	
51 - 65	Пороговый	3	удовлетворительно	
0 - 50	Первый	2	неудовлетворительно	Не зачтено

5 Материально-техническое, программное и учебно-методическое обеспечение дисциплины

5.1 Учебная литература

Основная учебная литература

1. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учеб. пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2019. — 223 с. — (Высшее образование). — www.dx.doi.org/10.12737/textbook_5cc15bb22f5345.11209330. - ISBN 978-5-16-014397-2. - URL: https://znanium.com/catalog/product/979415(дата обращения: 26.02.2019). – Текст: электронный.

Дополнительная учебная литература

1. Информационная безопасность и зашита информации : учебное пособие для направления подготовки 40.03.01 - Юриспруденция, специальности 40.05.02 - Правоохранительная деятельность, специальности 37.05.02 - Психология служебной деятельности, очной и заочной форм обучения / О. А. Панфилова, Д. Ю. Крюкова, А. Н. Наимов, В. В. Мухин ; Федер. служба исполн. наказаний, Вологод. ин-т права и экономики. - Вологда : ВИПЭ ФСИН России, 2018. - 59 с. - ISBN 978-5-94991-428-1. - URL: https://znanium.com/catalog/product/1229037(дата обращения: 26.02.2019). – Текст: электронный.

2. Шилов, А. К. Управление информационной безопасностью : учебное пособие / А. К. Шилов ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 120 с. - ISBN 978-5-9275-2742-7. –URL: https://znanium.com/catalog/product/1021744(дата обращения: 26.02.2019). – Текст: электронный.

5.2 Материально-техническое и программное обеспечение дисциплины

Учебные занятия по дисциплине проводятся в учебных аудиториях НФИ КемГУ

220 Учебная аудитория для проведения: - занятий лекционного типа; - семинарского (практического) типа; - групповых и индивидуальных консультаций; Специализированная (учебная) мебель: доска маркерно-меловая, столы, стулья. Оборудование для презентации учебного материала: *стационарное* - компьютер, проектор, доска интерактивная, акустическая система. Используемое программное обеспечение: MSWindows (MicrosoftImaginePremium 3 year по сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.), LibreOffice (свободно распространяемое ПО), антивирусное ПО ESETEndpointSecurity, лицензия №EAV-0267348511 до 30.12.2022 г.;MozillaFirefox (свободно распространяемое ПО), GoogleChrome (свободно распространяемое ПО), Opera(свободно распространяемое ПО), FoxitReader (свободно распространяемое ПО), WinDjView (свободно распространяемое ПО), Яндекс.Браузер (отечественное свободно распространяемое ПО). Интернет с обеспечением доступа в ЭИОС.	654027, Кемеровская область - Кузбасс, г. Новокузнецк, пр-кт Пионерский, д.13, пом.1
222 Учебная аудитория для проведения: - занятий семинарского (практического) типа; - групповых и индивидуальных консультаций; - текущего контроля и промежуточной аттестации. Специализированная (учебная) мебель: доска маркерно-меловая, столы, стулья. Оборудование для презентации учебного материала: *переносное* - ноутбук, проектор, экран. Используемое программное обеспечение: MSWindows (MicrosoftImaginePremium 3 year по сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.), LibreOffice (свободно распространяемое ПО), антивирусное ПО ESET EndpointSecurity, лицензия №EAV-0267348511 до 30.12.2022 г.;MozillaFirefox (свободно распространяемое ПО), GoogleChrome (свободно распространяемое ПО), Opera (свободно распространяемое ПО), FoxitReader (свободно распространяемое ПО), WinDjView (свободно распространяемое ПО), Яндекс.Браузер (отечественное свободно распространяемое ПО). Интернет с обеспечением доступа в ЭИОС.	654027, Кемеровская область - Кузбасс, г. Новокузнецк, пр-кт Пионерский, д.13, пом.1

5.3 Современные профессиональные базы данных и информационные справочные системы

Перечень СПБД и ИСС по дисциплине

Учебные материалы для студентов (Информатика). Режим доступа:https://studme.org/Учебные

Общероссийский информационная система – современная информационная система, предоставляющая российским и зарубежным ученым различные возможности в поиске научной информации по математике, физике, информационным технологиям и смежным наукам.Режим доступаhttp://www.mathnet.ru /

Единое окно доступа к образовательным ресурсам – свободный доступ к интегральному каталогу образовательных интернет-ресурсов и к электронной библиотеке учебно-методических материалов для общего и профессионального образования (Психология). Режим доступа: http://window.edu.ru/catalog/?p_rubr=2.2.77.2

6 Иные сведения и (или) материалы

6.1.Примерные темы письменных учебных работ

Тема 1. Введение в предмет. Угрозы информационной безопасности.

Перечислите четыре уровня защиты компьютерных и информационных ресурсов?

А. Предотвращение, обнаружение, ликвидация, восстановление.

Б. Предотвращение, описание, ликвидация, восстановление.

В. Предотвращение, обнаружение, ограничение, восстановление.

Что называют критическими данными?

А. Данные, которые требуют сохранения из-за вероятности нанесения умышленно-гоущерба.

Б. Данные, которые требуют защиты из-за вероятности нанесения ущерба, если произойдет случайное или умышленное раскрытие данных.

В. Данные, которые требуют уничтожения из-за вероятности нанесения случайного ущерба при раскрытии данных.

Основные меры защиты информационной безопасности?

А. Идентификация, аутентификация.

Б. Паролирование, кодирование.

В. Авторизация, дублирование.

Что понимается под надежностью компьютерных систем?

А. Способность системы восстанавливать информацию при отказах отдельных устройств.

Б. Отказ системы на вход не идентифицированного пользователя.

В. Свойство системы выполнять возложенные на нее задачи в определенных условиях эксплуатации.

Что такое идентификатор пользователя?

А. Номер пользователя в журнале учетных записей.

Б. Уникальная информация, позволяющая различать индивидуальных пользователей.

В. Пароль для входа в систему.

Тема 2. Основные понятия теории информационной безопасности.

Способы доступа к данным:

А. Прямой, обратный.

Б. Параллельный, прямой.

В. Последовательный, прямой.

Что такое межсетевой экран?

А. Средство разграничения доступа, служащие для защиты от внешних угроз.

Б. Средство разграничения доступа, служащее для защиты от внешних угроз и угроз со стороны пользователей других сегментов корпоративных сетей.

В. Средство защиты от угроз со стороны пользователей других сегментов корпоративных сетей.

Основные подходы к созданию отказоустойчивых систем:

А. Помехоустойчивое кодирование информации, параллельный доступ к информации.

Б. Простое резервирование, помехоустойчивое кодирование информации, создание Адаптивных систем.

В. Создание адаптивных систем, зеркальное дублирование информации, резервирование.

По времени восстановления информации методы дублирования делятся на:

А. Оперативные, неоперативные.

Б. Статические, динамические.

В. Кратковременные, долговременные.

Что такое отказоустойчивость компьютерных систем?

А. Свойство компьютерной системы сохранять работоспособность при отказах отдельных устройств, блоков, схем.

Б. Способность компьютерной системы сохранять информацию при сбоях.

В. Возможность дублирования информации на съемные носители.

Тема 3. Программно-технические методы защиты.

Средства, используемые для блокировки ошибочных операций:

А. Программные, аппаратные.

Б. Физические, технические.

В. Технические, аппаратнопрограммные.

Что такое аутентификация пользователей?

А. Метод, применяемый для подтверждения и проверки пользователей.

Б. Процедура, необходимая для входа в компьютерную систему.

В. Процесс входа в компьютерную систему.

Что такое информационная безопасность?

А. Меры по защите информации от не санкционированного доступа.

Б. Меры по восстановлению информации, ограничению доступа, обнаружению ошибок, предотвращению преступлений.

В. Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе.

Что такое криптография?

А. Наука о способах преобразования информации с целью защиты от не санкционированного доступа.

Б. Вид шифрования и кодировки информации.

В. Метод защиты информации.

Для чего используются CGI-процедуры?

А. Для статического отображения HTML-документов.

Б. Для распределения прав доступа к серверу.

В. Для динамического порождения HTML-документов.

Тема 4. Криптографические методы защиты.

Уровни защиты информации в Intranet:

А. Морально-этический, программно-технический, физический.

Б. Административный, процедурный, законодательный.

В. Протокольный, межсетевой, уровень фильтрации доступа.

Что такое криптология?

А. Шифрование / дешифрование информации.

Б. Наука, состоящая из криптографии и криптоанализа.

В. Применение криптографии на практике.

Какая кампания первой предложила технологию, позволяющую использовать пластиковые карты для расчетов в сети?

А.Visa.

Б. Master Card. В. Cyber Cash.

Что такое карта памяти?

А. Пластиковая карта с магнитной полосой с обратной стороны, которая считывается специальным устройством.

Б. Карта со встроенной микросхемой, содержащей устройство для записи/ считывания информации.

В. Специальные цифровые купоны и жетоны.

Тема 5. Организационно-правовые методы информационной безопасности.

Что такое вскрытие шифра?

А. Процесс получения защищаемой информации.

Б. Процесс получения защищаемой информации из шифрованного сообщения со знанием примененного шифра.

В. Процесс получения защищаемой информации из шифрованного сообщения без предварительного знания примененного шифра.

Какие протоколы используются для квантово-криптографических систем?

А. Протокол первичной квантовой передачи, протокол исправления ошибок в битовых последовательностях, протокол оценки утечки к злоумышленнику информации о ключе, протокол усиления секретности и формирования итогового ключа.

Б. Протокол вторичной квантовой передачи, протокол исправления ошибок в данных, протокол оценки утечки информации, протокол уменьшения секретности ключа.

В. Протокол квантовой передачи, протокол битовых последовательностей, протокол оценки утечки к злоумышленнику информации о ключе, протокол формирования итогового ключа.

Методологии шифрования:

А. Симметричная, асимметричная. Б. Прямая, зеркальная.

В. Открытая, закрытая.

Для чего используется электронная подпись?

А. Позволяет проверять целостность данных, но не обеспечивает их конфиденциальность.

Б. Позволяет проверять целостность данных, и обеспечивает их конфиденциальность.

В. Не позволяет проверять целостность данных, но обеспечивает их конфиденциальность.

Что такое компьютерный вирус?

А. Небольшие исполняемые программы, обладающие свойством распространения и репликации в компьютерной системе.

Б. Информационные системы, обладающие свойством распространения и самовоспроизведения.

В. Программные комплексы, изменяющие или уничтожающие программное обеспечение, не обладающие свойством самовоспроизведения.

По способу заражения среды обитания компьютерные вирусы делятся на:

А. Резидентные, нерезидентные.

Б. Целостные, частичные.

В. Оперативные, неоперативные.

Тема 6. Роль стандартов в обеспечении информационной безопасности.

По степени опасности для информационных ресурсов компьютерные вирусы делятся на:

А. Безопасные, частично опасные, опасные.

Б. Безвредные, частично опасные, очень опасные.

В. Безвредные, опасные, очень опасные.

Что такое макровирус?

А. Вредительская программа, имеющая большую среду обитания.

Б. Вредительская программа, написанная на макроязыках, встроенных в текстовые редакторы, электронные таблицы и др.

В. Вредительская программа, заражающая программно-аппаратные средства.

Какие методы из перечисленных являются методами обнаружения вирусов?

А. Сканирование, вакцинирование программ, обнаружение изменений.

Б. Сканирование, шифрование, криптоанализ.

В. Эвристический анализ, криптозащита, аутентификация.

Для каких целей применяют антивирусные средства?

А. Для создания, копирования, изменения вирусов.

Б. Для обнаружения, блокирования работы вирусов, устранения последствий воздействия вирусов.

В. Для обнаружения и удаления вирусов.

Что включают организационные методы защиты информации?

А. Меры, мероприятия и действия, которые должны осуществлять должностные лица в процессе создания и эксплуатации компьютерных систем для обеспечения заданного уровня безопасности информации.

Б. Меры, мероприятия и действия, которые должен осуществлять персонал в процессе эксплуатации компьютерных систем.

В. Действия, которые должен осуществлять разработчик в процессе создания компьютерных систем для обеспечения заданного уровня безопасности информации.

Доклад

а) Тематика устных докладов

Тема 1. Введение в предмет. Угрозы информационной безопасности.

Политика информационной безопасности предприятия.

Нормативно-правоваябазаобеспеченияинформационнойбезопасностипредприятия.

Содержание основных законов Российской Федерации в сфере компьютерного права.

Законодательная база РФ по вопросам защиты информации.

Комплексный подход к обеспечению информационной безопасности.

Тема 2. Основные понятия теории информационной безопасности.

Законодательные и нормативные акты РФ о предпринимательской деятельности.

Машинное представление информации.

Виды и формы представления информации.

Информация как объект правасобственности.

Информация как коммерческая тайна.

Информация как рыночный продукт.

Элементы и объекты защиты в АС.

Тема 3. Программно-технические методы защиты.

Основные виды вирусов и схемы ихфункционирования.

Обнаружение вирусов и меры по защите и профилактике

Основные меры защиты от вирусов.

Программно-технические меры обеспечения информационной безопасности.
Обеспечение информационной безопасности средствами Windows7.

Тема 4. Криптографические методы защиты.
Безопасное хранение данных на основе шифрования.
Американский стандарт шифрования данных DES.
Стандарт шифрования данных ГОСТ28147-89.
Система цифровой телефонии.
Системы шифрования с открытыми ключами.

Тема 5. Организационно-правовые методы информационной безопасности.
Цифровые подписи на основе шифросистем с открытым и ключами.
Комплексный подход к обеспечению информационной безопасности:
Механические системы защиты

Тема 6. Роль стандартов в обеспечении информационной безопасности.
Политика информационной безопасности предприятия.
Нормативно-правовая база обеспечения информационной безопасности предприятия. Содержание основных законов Российской Федерации в сфере компьютерного права.
Законодательная база РФ по вопросам защиты информации.
Комплексный подход к обеспечению информационной безопасности.
Законодательные и нормативные акты РФ о предпринимательской деятельности.

Критерии оценивания
Критериями оценивания доклада являются полнота раскрытия темы, степень ее проработанности, последовательность изложения материала; умения студента самостоятельно работать с литературой и информационно-электронными ресурсами, аргументированно и ясно строить речь, эффектно и наглядно представлять содержание результатов своей работы, а также владения навыками дискуссии и публичной защиты результатов своих исследований.

Описание шкалы оценивания
Устные доклады оцениваются по шкале «зачтено»/«не зачтено».
«Зачтено» выставляется в случае, если студент свободно излагает материал по заданному вопросу, опираясь при этом на литературные и другие дополнительные источники, отвечает на дополнительные уточняющие вопросы преподавателя и аудитории студентов, приводит практические примеры, аргументированно отстаивает свою точку зрения; во время доклада использует раздаточный материал и (или)презентацию.
«Не зачтено» выставляется в случае, если в изложении наблюдаются значительные пробелы в знании материала и (или) студент не отвечает на дополнительные уточняющие вопросы и (или) не использует иллюстративный материал.

6.2. Примерные вопросы и задания / задачи для промежуточной аттестации

Таблица 9 – Примерные теоретические вопросы и практические задания к экзамену

Разделы и темы	Примерные теоретические вопросы	Примерные

		практические задания
Тема 1. Информатизация общества и информационная безопасность		
	1. Сформулируйте личностные характеристики хакера. 2. Что понимается под «безопасностью информации», а что определяет термин «защита информации»? 3. Дайте определение политики безопасности. 4. На каких уровнях управления организацией разрабатывается политика безопасности? 5. Для каких целей строится модель нарушителя? 6. Перечислите некоторые типы конфликтов в организации. 7. Назовите самое простое средство социальной инженерии. 8. Какие категории пользователей могут нанести максимальный вред информационной системе?	Для одно алфавитного метода с задаваемым смешением выполнить шифрование с произвольным смещением.
Тема 2. Нормативно-правовое обеспечение информационной безопасности в Российской Федерации.		
	9. Что следует понимать под «правовым режимом информации»? 10. Назовите несколько наиболее важных законов, регламентирующих информационные отношения в обществе. 11. Поясните разницу между собственником, владельцем и пользователем информации. 12. Перечислите органы защиты государственной тайны. 13. Какая информация, по закону, не может быть закрытой? 14. Перечислите основные нормативные документы по защите информации. 15. Укажите категории информации ограниченного доступа. 16. Поясните смысл категории «коммерческая тайна».	Для одного алфавитного метода с задаваемым смешением выполнить дешифрование зашифрованный шифром Цезаря текст.
Тема 3. Организация противодействия компьютерной преступности.		
	17. Каковы структурные особенности	Проверить на

	УК РФ в области компьютерной преступности? 18. Перечислите базовые классификационные признаки угроз информационной безопасности в автоматизированных системах. 19. Укажите основные причины утечки информации на объектах информатизации. 20. Что понимается под несанкционированным доступом в информационную систему? 21. Перечислите категории компьютерных преступников. 22. Назовите виды компьютерной преступности.Способность разрабатывать и реализовывать программы, направленные на предупреждение нарушений и отклонений в социальном и личностном статусе, психическом развитии сотрудников, военнослужащих и иных лиц, рисков асоциального поведения, профессиональных рисков, профессиональной деформации с учетом развития в современном мире компьютерной преступности. 23. Укажите способы совершения компьютерных преступлений. 24. Какое максимальное наказание и по какой статье может назначить суд за компьютерное преступление? 25. Как следует опечатывать ПЭВМ так, чтобы исключить возможность работы с ними? 26. Укажите типичные следственные ситуации при расследовании компьютерных преступлений.	простоту два произвольных целых числа разрядностью5.
Тема 4. Типовые решения по безопасности компьютерных сетей.		
	27. Что такое протокол TCP/IP? 28. Что включает в себя понятие сокет? 29. Сформулируйте вопросы, учитывающие возможные последствия подключения к Internet. 30. В чем состоит фундаментальная	Задан интервал вида [x, x + L]. Вычислить количество П(x, L) простых чисел в интервале и сравнить с величиной L/1п(x).

	проблема безопасности Internet? 31. Назовите основные модели безопасного подключения к Internet. 32. Дайте определение межсетевого экрана. 33. Укажите две базовые политики межсетевого экрана.	При каких условиях П(x, L)/L близко к 1/1n(x) при заданных x = 2000, L= 500, количество простых чисел для деления 5-15, количество оснований1-2?
Тема 5. Организация противодействия вредоносным программам.		
	34. Каким документом регламентирован термин «вредоносные программы»? 35. Какие виды вредоносных программ существуют? 36. Чем отличаются компьютерные вирусы от троянских программ? 37. Какие меры наиболее эффективны против захватчиков паролей? 38. Перечислите средства нейтрализации вирусов (вредоносных программ). 39. Какие потери (затраты) и на что именно несут организации в связи с существованием явления «вредоносная программа»? 40. Как вы думаете, что такое потери репутации и как они могут быть связаны с вредоносными программами? 41. Укажите способы тиражирования антивирусного обеспечения. 42. Назовите известные вам антивирусные программы. 43. Какие вредоносные программы, на ваш взгляд, являются самыми опасными для информационной системы?	Найти в интервале (1000, 1000 + 300) все простые числа. Пусть L(i) - разность между двумя соседними простыми числами. Построить гистограмму для L(i). Вычислить выборочное среднее Lсред. Сравнить с величиной 1n(x), где x - середина интервала. Задано: количество простых чисел для деления 5-20, количество оснований1-3.
Тема 6. Криптография как метод обеспечения информационной безопасности.		
	44. Что понимается под термином управление криптографическими ключами? Какова основная цель и основные задачи управления ключами? 45. В чем, на ваш взгляд, отличие жизненного цикла секретных и открытых криптографических ключей? 46. Изложите в общих чертах существо сертификации открытых ключей. 47. Каким образом распространяются открытые ключи в криптосистемах?	В интервале (500, 500 + 200) построить график относительного количества натуральных чисел, проходящих «решето Эратосфена», т.е. не делящихся на первые к простых. Расчет производится для всех

	48. Укажите преимущества симметричных криптосистем, определившие их как национальные стандарты государств. 49. Что такое удостоверяющий центр? 50. Для чего применяются хэш-функции? 51. Какие классы преобразования распространены в симметричных системах? 52. Для чего необходима электронная подпись?	k<=10.

Составитель: Гета М.Р., канд. юрид. наук, доцент