МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кемеровский государственный университет»
Кузбасский гуманитарно-педагогический институт
федерального государственного бюджетного образовательного учреждения
высшего образования
«Кемеровский государственный университет»
Факультет информатики, математики и экономики

УТВЕРЖДАЮ
Декан А.В. Фомина
9 февраля 2023 г

Рабочая программа дисциплины

Б1.О.16 Информационная безопасность
Код, название дисциплины

Направление подготовки
09.03.03 Прикладная информатика
Код, название направления

Направленность (профиль) подготовки
Прикладная информатика в экономике

Программа бакалавриата

Квалификация выпускника
бакалавр

Форма обучения
Очно-заочная

Год набора 2020

Новокузнецк 2023

Оглавление

1 Цель дисциплины. 3
1.1 Формируемые компетенции 3
1.2 Индикаторы достижения компетенций 3
1.3 Знания, умения, навыки (ЗУВ) по дисциплине 4
2 Объём и трудоёмкость дисциплины по видам учебных занятий. Формы промежуточной аттестации. 5
3. Учебно-тематический план и содержание дисциплины. 5
3.1 Учебно-тематический план 5
3.2. Содержание занятий по видам учебной работы 6
4 Порядок оценивания успеваемости и сформированности компетенций обучающегося в текущей и промежуточной аттестации. 9
5 Материально-техническое, программное и учебно-методическое обеспечение дисциплины. 10
5.1 Учебная литература 10
5.2 Материально-техническое и программное обеспечение дисциплины. 11
5.3 Современные профессиональные базы данных и информационные справочные системы 14
6 Иные сведения и (или) материалы 14
6.1.Примерные темы письменных учебных работ 14
6.2. Примерные вопросы и задания / задачи для промежуточной аттестации 15

1 Цель дисциплины.

В результате освоения данной дисциплины у обучающегося должны быть сформированы компетенции основной профессиональной образовательной программы бакалавриата (далее - ОПОП):

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

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 *(универсальная, общепрофессиональная, профессиональная)*	Наименование категории (группы) компетенций	Код и название компетенции
общепрофессиональная		ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

1.2 Индикаторы достижения компетенций

Таблица 2 – Индикаторы достижения компетенций, формируемые дисциплиной

Код и название компетенции	Индикаторы достижения компетенции по ОПОП	Дисциплины и практики, формирующие компетенцию ОПОП
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК 3.1 Разрабатывает меры защиты информации на основе требований информационной безопасности и нормативно-правовой базы ОПК 3.2 Осуществляет ведение базы данных, устанавливает и настраивает СУБД ОПК 3.3 Настраивает параметры ИС и тестирует результаты настройки ОПК 3.4 Осуществляет техническое сопровождение информационных систем в процессе эксплуатации	Б1.О.02 Введение в профессиональную деятельность Б1.О.06 Информационные системы и технологии Б1.О.15 Правовое обеспечение внедрения и эксплуатации информационных систем **Б1.О.16 Информационная безопасность** Б1.О.18 Базы данных Б2.О.03(У) Учебная практика. Технологическая (проектно-технологическая) практика Б3.01(Д) Выполнение и защита выпускной

Код и название компетенции	Индикаторы достижения компетенции по ОПОП	Дисциплины и практики, формирующие компетенцию ОПОП
		квалификационной работы

1.3 Знания, умения, навыки (ЗУВ) по дисциплине

Таблица 3 – Знания, умения, навыки, формируемые дисциплиной

Код и название компетенции	Индикаторы достижения компетенции, закрепленные за дисциплиной	Знания, умения, навыки (ЗУВ), формируемые дисциплиной
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК 3.1 Разрабатывает меры защиты информации на основе требований информационной безопасности и нормативно-правовой базы	Знать: • базовые понятия информационной безопасности; классификацию угроз уязвимостей; • нормативно-правовую базу в области защиты информации; • основные понятия и методы организационно-правового, программно-аппаратного, криптографического обеспечения информационной безопасности; • методики построения систем защиты информации Уметь: • моделировать угрозы и уязвимости информационной безопасности; • выделять источники информации, объекты защищаемой информации; • формировать требования к построению безопасной системы; • определять функциональные задачи и требования Владеть: • методами организационно-правового, программно-аппаратного, криптографического обеспечения информационной безопасности; • методами и методиками построения систем защиты информации; • программными продуктами для оценки риска информационной безопасности; • программными средствами обеспечения информационной безопасности;

Код и название компетенции	Индикаторы достижения компетенции, закрепленные за дисциплиной	Знания, умения, навыки (ЗУВ), формируемые дисциплиной
		• протоколами аутентификации, распределения ключей, электронной подписи и финансовой криптографии

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
	ОЗФО
1 Общая трудоемкость дисциплины	144
2 Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	
Аудиторная работа (всего):	44
в том числе:	
лекции	8
практические занятия, семинары	36
практикумы	
лабораторные работы	
в интерактивной форме	
в электронной форме	
Внеаудиторная работа (всего):	64
в том числе, индивидуальная работа обучающихся с преподавателем	64
подготовка курсовой работы /контактная работа	
групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие групповую или индивидуальную работу обучающихся с преподавателем)	
творческая работа (эссе)	
3 Самостоятельная работа обучающихся (всего)	
4 Промежуточная аттестация обучающегося – экзамен, 4 семестр	36

3. Учебно-тематический план и содержание дисциплины.

3.1 Учебно-тематический план

Таблица 5 - Учебно-тематический план очной формы обучения

№ недели п/п	Разделы и темы дисциплины по занятиям	Общая трудоёмкость *(всего час.)*	Трудоемкость занятий (час.)			Формы текущего контроля и промежуточной аттестации успеваемости
			ОЗФО			
			Аудиторн. занятия		СРС	
			лекц.	практ.		

№ недели п/п	Разделы и темы дисциплины по занятиям	Общая трудоёмкость *(всего час.)*	Трудоемкость занятий (час.)			Формы текущего контроля и промежуточной аттестации успеваемости
			ОЗФО			
			Аудиторн. занятия		СРС	
			лекц.	практ.		
	1. Основы информационной безопасности	24	4	8	12	
1-2	1.1 Базовые понятия и нормативно-правовая база обеспечения информационной безопасности	8	1	2	5	Тест №1
3-4	1.2 Модели безопасности	16	1	6	9	Реферат
	2. Меры защиты информации	60	10	20	30	
5-6	2.1 Организационно-правовое обеспечение информационной безопасности	12	1	4	7	Тест №2
7-10	2.2 Криптографические методы защиты информации	22	1	8	13	Тест №3 Индивидуальное задание №1-2
11-12	2.3 Программно-аппаратное обеспечение информационной безопасности	16	1	4	11	Реферат
13-14	2.4 Защита информации в IP-сетях	10	1	4	5	Индивидуальное задание №3
	3 Системы защиты информации	24	4	8	12	
15-16	3.1 Анализ и управление рисками в информационной безопасности	8	1	4	3	Тест №4
17-18	3.2 Проектирование систем защиты информации	16	1	4	11	Индивидуальное задание №4
19	Промежуточная аттестация - экзамен	36				экзамен
	Всего:	144	8	36	64	

3.2. Содержание занятий по видам учебной работы

Таблица 6 – Содержание дисциплины

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
Содержание лекционного курса		
1	*Основы информационной безопасности*	
1.1	Базовые понятия и нормативно-правовая база обеспечения информационной	*Базовые понятия: информация, защищаемая информация, системы обработки информации, информационные ресурсы, угрозы, источники угроз безопасности, уязвимости. Направления защиты информации. Средства и способы*

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
	безопасности	*защиты информации. Классификации угроз уязвимости. Объекты защиты.* *Идентификация, аутентификация, управление доступом. Защита от несанкционированного доступа. Политика безопасности.* *Нормативные акты, регламентирующие деятельности в области защиты информации: ФЗ «Об информации, информационных технологиях и о защите информации», отечественные и международные стандарты в области защиты информации, руководящие документы ФСТЭК.*
1.2	Модели безопасности	*Сущность, объект и субъект защиты информации. Доступы. Схема контроля доступа. Модели контроля доступа: абстрактные модели дискреционного контроля доступа, избирательного контроля доступа, мандатного контроля доступа, контроля доступа к создаваемым объектам, вероятностная и процессная модель контроля доступа. Методы ролевого и сессионного контроля доступа.* *Общий подход математического моделирования угроз безопасности. Моделирование угроз безопасности. Моделирование надежностных параметров и характеристик безопасности. Моделирование потенциального нарушителя, реализуемости и реализации реальных угроз атак*
2	*Меры защиты информации*	
2.1	Организационно-правовое обеспечение информационной безопасности	*Правовые средства обеспечения безопасности информации.* *Организационное обеспечение информационной безопасности РФ.* *Организационно-правовые проблемы международной информационной безопасности.* *Правовые режимы обеспечения безопасности информации ограниченного доступа.* *Особенности организационно-правового обеспечения защиты информационных систем.* *Юридическая ответственность за правонарушения в информационной сфере.*
2.2	Основные положения, методы и схемы криптографии	*Криптосинтез. Криптоанализ. Криптология. Критографическая система. Криптографический протокол. Криптографическая стойкость.* *Ключ. Шифр. Зашифрование. Расшифрование. Открытый текст. Шифртекст. Блочные и поточные шифры. Стеганография.* *Криптосистемы с секретным ключом. Криптосистемы с открытым ключом.* *Теория Шеннона. Схема Фейстеля. Алгоритм шифрования DES. Режимы работы блочных шифров. ГОСТ 28147-89. Шифр AES. Имитостойкость и помехоустойчивость.* *Симметричные и асимметричные шифры. Схема Диффи-Хеллмана. Математические основы асимметричной*

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
		криптографии. Шифр Шамира. Шифр Эль-Гамаля. Шифр RSA. *Перспективные направления развития.* *Нормативные документы.*
2.3	Криптографические протоколы. Хэширование. Электронно-цифровая подпись	*Схемы электронной подписи. Схемы построения хэш-функций. Схемы построения псевдослучайных генераторов.* *Протоколы аутентификации. Протоколы распределения ключей. Разновидности протоколов электронной подписи.* *Протоколы финансовой криптографии.*
2.4	Программно-аппаратное обеспечение информационной безопасности	*Основания теории и практики защиты программного обеспечения: элементы теории алгоритмов, элементы сложности вычислений.* *Методы обеспечения технологической и эксплуатационной безопасности программного обеспечения: классификация вредоносных программ, защита от вредоносных программ, методы тестирования программного обеспечения на его защищенность, методы защиты программ от несанкционированного исследования и копирования.* *Средства, системы и комплексы защиты программного обеспечения. Исследование программного обеспечения на предмет отсутствия недекларированных возможностей.*
2.5	Защита информации в IP-сетях	*Протокол защиты электронной почты S/MIME. Протоколы SSL и TLS. Протоколы IPSec и распределение ключей. Межсетевые экраны.*
3	*Системы защиты информации*	
3.1	Анализ и управление рисками в информационной безопасности	*Понятие риска в сфере ИБ. Управление рисками. Модель безопасности с полным перекрытием.* *Управление информационной безопасностью.* *Методики построение систем защиты информации. Методики и программные продукты для оценки рисков.*
3.2	Проектирование систем защиты информации	*Формирование требований к построению безопасной системы: формирование требований для систем защиты информации базового и повышенного уровня защиты. Построение безопасных отказоустойчивых систем.* *Стадии и задачи проектирование. Определение функциональных задач и требований систем защиты информации. Экономическое обоснование проектных решений. Оценка производительности.*
Содержание практических занятий		
1	*Основы информационной безопасности*	
1.1	Объекты защиты	*Определение защищаемой информации на объекте. Определение источника информации, направления защиты информации. Определение объекта защиты.*
1.2	Моделирование контроля доступа	*Построение одной из моделей контроля доступа. Анализ моделей контроля доступа для объекта.*

№ п/п	Наименование раздела, темы дисциплины	Содержание занятия
1.3	Моделирование угроз безопасности	*Построение системы состояний случайного процесса модели угроз безопасности. Моделирование системы с отказами.*
1.4	Расчет эксплуатационных характеристик безопасности	*Расчет сложности реализации угрозы безопасности. Расчет остаточной сложности для нарушителя. Определение вероятности реализации угрозы*
2	*Меры защиты информации*	
2.1	Организационные меры защиты	*Разработка организационной политики безопасности*
2.2	Правовые меры защиты	*Решение практических задач по определению юридической ответственности и мер правовой защиты*
2.3	Простейшие криптографические шифры	*Шифры подстановки. Шифры перестановки. Комбинированные шифры*
2.4	Блочные шифры	*Алгоритм шифрования DES. ГОСТ 28147-89. Шифр AES.*
2.5	Асимметричная криптография	*Шифр Шамира. Шифр Эль-Гамаля. Шифр RSA.*
2.6	Криптографические протоколы	*Протоколы аутентификации. Протоколы распределения ключей.*
2.7	Защита от вредоносных программ	*Определение и классификация вредоносных программ*
2.8	Исследование программного обеспечения	*Тестирование программного обеспечения на его защищенность, защита программ от несанкционированного исследования и копирования.*
2.9	Использование сканеров безопасности для получения информации о хостах в сети	*Определение работающих сетевых приложений с помощью сетевого сканера безопасности*
2.10	Использование цифровых сертификатов	*Ознакомление с порядком использования цифровых сертификатов*
3	*Системы защиты информации*	
3.1	Риски информационной безопасности	*Определение и оценка рисков информационной безопасности.*
3.2	Требования к системе защиты базового уровня	*Определение функциональных задач и требований системы защиты информации базового уровня защиты*
3.3	Требования к системе защиты повышенного уровня	*Определение функциональных задач и требований системы защиты информации повышенного уровня защиты*
3.4	Экономическое обоснование проекта	*Построение проектного решения и его экономическое обоснование*
	Промежуточная аттестация - *экзамен*	

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 таблице 7.

Таблица 7 - Балльно-рейтинговая оценка результатов учебной работы обучающихся по видам (БРС)

Учебная работа (виды)	Сумма баллов	Виды и результаты учебной работы	Оценка в аттестации	Баллы (18 недель)
Текущая учебная работа в семестре (Посещение занятий по расписанию и выполнение заданий)	**60**	Практические работы (отчет о выполнении лабораторной работы) (18 работ).	**0,75 балл** - посещение 1 практического занятия и выполнение работы на 51-65% **1,5 балла** – посещение 1 занятия и существенный вклад на занятии в работу всей группы, самостоятельность и выполнение работы на 85,1-100%	13 - 27
		Индивидуальные работы (отчет о выполнении) (4 работы)	**За одну ИР :** **2 балла** (выполнено 66 - 85% заданий) **3 балла** (выполнено 86 - 100% заданий)	8 - 12
		Тесты (4 работы)	**За один тест:** **2 баллов** (выполнено 51 - 65% заданий) **4 балла** (выполнено 86 - 100% заданий)	8-16
		Реферат (по разделу 1 или 2 на выбор)	**2 балла** (пороговое значение) **5 баллов** (максимальное значение)	2 - 5
Итого по текущей работе в семестре				31 - 60
Промежуточная аттестация (экзамен)	40 (100% /баллов приведенной шкалы)	Теоретический вопрос (2 вопроса).	**7,5 балла** (пороговое значение) **15 баллов** (максимальное значение)	15 - 30
		Решение задачи 1.	**5 балла** (пороговое значение) **10 баллов** (максимальное значение)	5 - 10
Итого по промежуточной аттестации (экзамену)				(51 – 100% по приведенной шкале) 20 – 40 б.
Суммарная оценка по дисциплине: Сумма баллов текущей и промежуточной аттестации				51 – 100 б.

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

5.1 Учебная литература

Основная учебная литература

1. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/434171 (дата обращения: 02.12.2019).
2. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2019. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/433715 (дата обращения:

02.12.2019).

Дополнительная учебная литература

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для академического бакалавриата / И. Н. Васильева. — Москва : Издательство Юрайт, 2019. — 349 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-02883-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/433610 (дата обращения: 02.12.2019).
2. Запечников, С. В. Криптографические методы защиты информации : учебник для академического бакалавриата / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2019. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/433133 (дата обращения: 02.12.2019).
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2019. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/437163 (дата обращения: 02.12.2019).
4. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2019. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/432966 (дата обращения: 02.12.2019).

5.2 Материально-техническое и программное обеспечение дисциплины.

Учебные занятия по дисциплине проводятся в учебных аудиториях НФИ КемГУ.

Таблица 8 – Материально-техническое и программное обеспечение аудиторных занятий и самостоятельной работы

Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы	Перечень основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом

410 Учебная аудитория (мультимедийная) для проведения: - занятий лекционного типа;	Специализированная (учебная) мебель: доска меловая, кафедра, моноблоки аудиторные. Оборудование: стационарное - компьютер, экран, проектор. 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), Яндекс.Браузер (отечественное свободно распространяемое ПО). Интернет с обеспечением доступа в ЭИОС.	654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19
501 Компьютерный класс. Учебная аудитория (мультимедийная)для проведения: - занятий семинарского (практического) типа; - групповых и индивидуальных консультаций; - текущего контроля и промежуточной аттестации;	Специализированная (учебная) мебель: доска меловая, кафедра, столы компьютерные, стулья. Оборудование для презентации учебного материала:стационарное - компьютер преподавателя, экран, проектор. Оборудование: стационарное - компьютеры для обучающихся (17 шт.). 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), BloodshedDevC++ 4.9.9.2 (свободно распространяемое ПО), FoxitReader (свободно распространяемое ПО), Firefox 14 (свободно распространяемое ПО), Яндекс.Браузер (отечественное свободно распространяемое ПО), Java (бесплатная версия), MicrosoftVisualStudio	654079, Кемеровская область, г. Новокузнецк, пр-кт Металлургов, д. 19

	(MicrosoftImaginePremium 3 year по сублицензионному договору № 1212/КМР от 12.12.2018 г. до 12.12.2021 г.) Интернет с обеспечением доступа в ЭИОС.	

5.3 Современные профессиональные базы данных и информационные справочные системы.

Перечень СПБД и ИСС по дисциплине

1. CITForum.ru - on-line библиотека свободно доступных материа-лов по информационным технологиям на русском языке - http://citforum.ru
2. Научная электронная библиотека eLIBRARY.RU – крупнейший российский информационный портал в области науки, технологии, ме-дицины и образования, содержащий рефераты и полные тексты - www.elibrary.ru
3. Единое окно доступа к образовательным ресурсам - http://window.edu.ru/

6 Иные сведения и (или) материалы.

6.1.Примерные темы письменных учебных работ

Темы реферата

Раздел 1 Основы информационной безопасности

1. Схемы контроля на основе атрибутов и матрицы доступа
2. Вероятностная модель контроля доступа
3. Процессная модель контроля доступа
4. Идентификация ролей и сессий
5. Сравнение моделей контроля доступа
6. Источники исходных данных для моделирования угроз безопасности
7. Моделирование угроз атак с отложенной реализацией
8. Сканеры безопасности
9. Моделирование угрозы отказов системы безопасности
10. Определение надежностных параметров угрозы уязвимости в общем виде
11. Математическая модель потенциального нарушителя

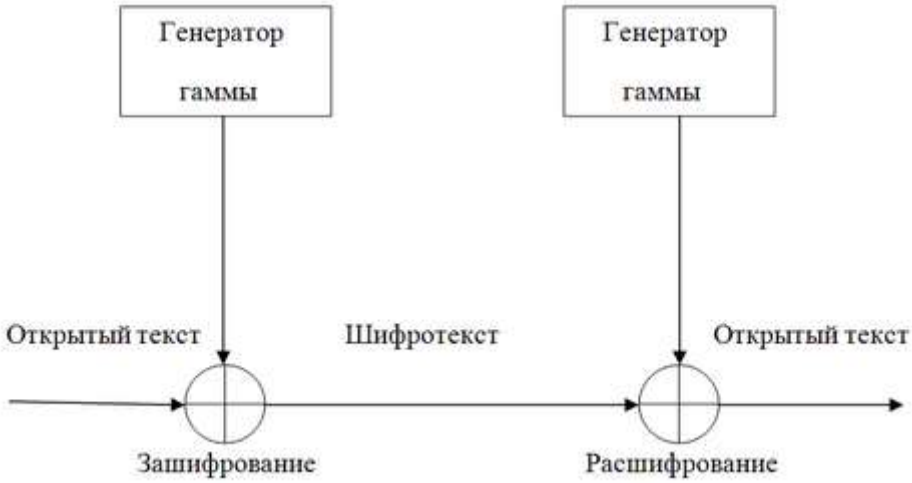
Раздел 2. Меры защиты информации

12. Фаззинг программ
13. Обфускация программ
14. Способы встраивания защитных механизмов в программное обеспечение
15. Манипуляция с кодом программы для защиты программы от несанкционированного доступа
16. Методы противодействия динамическими способами снятия защиты программ от копирования
17. Методы обнаружения уязвимостей операционных систем
18. Статический анализ исходных текстов программ
19. Динамический анализ исходных текстов программ
20. Сертификация средств защиты информации по требованиям безопасности информации

Темы индивидуального задания

Индивидуальное задание №1

1. Программно реализовать простейший режим гаммирования для поточных шифров.



2. Программно реализовать любой блочный шифр из предложенных:
   Алгоритм шифрования DES.
   ГОСТ 28147-89.
   Шифр AES.

Индивидуальное задание №2

1. Реализовать любой из шифров замены:
   Одноразовый блокнот
   Шифр Виженера
   Шифр Хилла
   Шифр Плейфера
2. Реализовать один из методов криптоанализа

Индивидуальное задание №3

1. Опишите настройки межсетевого экрана Windows Server
2. Определите новые разрешающие правила
3. Запретите отправку ICMP-пакетов на один из узлов
4. Настройте ведение журнала

Индивидуальное задание №4

1. Постройте модели угроз информационной безопасности для объекта
2. Оцените риски информационной безопасности
3. Составьте требования защиты информационной безопасности на базовом уровне
4. Рассчитайте экономическое обоснование
5. Составьте оценку производительности

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
1. Основы информационной безопасности		
1.1 Базовые понятия и нормативно-правовая база обеспечения информационной безопасности	1. Классификация средств и способов защиты информации 2. Защищаемая информация. Объекты защиты 3. Регламентирующие	Классифицировать защищаемую информацию Определить объекты защиты на предприятии

	нормативные акты 4. Международные стандарты в области защиты информации	
1.2 Модели безопасности	5. Общая схема контроля доступа 6. Абстрактная модель дискреционного контроля доступа 7. Абстрактная модель избирательного контроля доступа 8. Абстрактная модель мандатного контроля доступа 9. Модель ролевого доступа 10. Моделирование угроз безопасности 11. Математическое моделирование угроз безопасности 12. Моделирование потенциального нарушителя	Построить модель контроля доступа Построить систему состояний случайного процесса для модели угрозы безопасности Определить вероятность реализации угрозы Рассчитать сложность реализации угрозы безопасности
2. Меры защиты информации		
2.1 Организационно-правовое обеспечение информационной безопасности	13. Правовые средства защиты информации 14. Информация ограниченного доступа. Правовые режимы обеспечения безопасности 15. Юридическая ответственность за правонарушения 16. Организационное обеспечение безопасности	Определить юридическую ответственность за несанкционированный доступ к государственной тайне Определить юридическую ответственность за распространение вредоносного ПО Определить организационные меры защиты для ИСПДн отдела кадров
2.2 Криптографические методы защиты информации	17. Криптография. Криптоанализ. Криптология 18. Стеганография 19. Криптосистемы с секретным ключом 20. Криптосистемы с открытым ключом 21. Алгоритмы на основе сети Фейстеля 22. Блочные шифры 23. Имитостойкость шифра 24. Асимметричная криптография 25. Шифр AES 26. Шифр RSA 27. Электронно-цифровая подпись 28. Хэш-функции 29. Псевдослучайные генераторы 30. Протоколы	Зашифровать открытый текст методом перестановки Зашифровать открытый текст методов подстановки Определить наличие коллизий в хэш-функции Определить протокол распределения ключей для коллектива из 10 человек Реализовать алгоритм шифрования

	аутентификации 31. Протоколы распределения ключей 32. Протоколы финансовой криптографии	
2.3 Программно-аппаратное обеспечение информационной безопасности	33. Классификация вредоносных программ 34. Методы тестирования программного обеспечения на его защищенность 35. Защита программ от несанкционированного исследования и копирования 36. Средства защиты программного обеспечения	Разработать меры защиты от несанкционированного копирования Определить вредоносное ПО
2.4 Защита информации в IP-сетях	37. Межсетевые экраны 38. Протоколы защиты электронной почты 39. Распределение ключей по сети	Определить работающие сетевые приложения Определить распределение ключей
3. Системы защиты информации		
3.1 Анализ и управление рисками в информационной безопасности	40. Понятие риска в сфере информационной безопасности 41. Управление информационной безопасностью 42. Методики оценки рисков	Оценить риск для информационной системы отдела кадров Оценить риск для ИСПДн больницы
3.2 Проектирование систем защиты информации	43. Требования к построению безопасной системы 44. Построение безопасных отказоустойчивых систем 45. Стадии и задачи проектирования систем защиты информации 46. Оценка производительности	Составить требования к системе защиты информации государственного предприятия Составить требования к системе защиты информации повышенного уровня защиты для интернет-площадки

Составитель (и): Штейнбрехер О.А., канд. техн. наук, доцент кафедры ИВТ
(*фамилия, инициалы и должность преподавателя (ей)*)