Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Щёкина Вера Викторовна
Должность: Ректор
Дата подписания: 10.10.2022 08:25:01
Уникальный программный ключ:
a2232a5515[illegible]

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Благовещенский государственный педагогический университет»

ОСНОВНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
Рабочая программа дисциплины

УТВЕРЖДАЮ
И.о. Декана физико-математического факультета ФГБОУ ВО «БГПУ»

_____ **О.А. Днепровская**
«22» мая 2019 г.

Рабочая программа дисциплины
МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки
44.03.05 ПЕДАГОГИЧЕСКОЕ ОБРАЗОВАНИЕ
(с двумя профилями подготовки)

Профиль
«ИНФОРМАТИКА»

Профиль
«МАТЕМАТИКА»

Уровень высшего образования
БАКАЛАВРИАТ

Принята на заседании кафедры
информатики и методики преподавания информатики
(протокол № __9__ от «15» мая 2019 г.)

Благовещенск 2019

СОДЕРЖАНИЕ

1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1 Цель дисциплины: формирование систематизированных знаний и навыков в области средств защиты информации.

1.2 Место дисциплины в структуре ООП: Дисциплина «Методы и средства защиты информации» относится к дисциплинам по выбору вариативной части дисциплин (модулей) (Б1.В.11). Для освоения дисциплины студенты используют знания и умения, сформированные в процессе освоения математических дисциплин, дисциплин: «Информационные технологии», «Операционные системы и компьютерные сети», «Архитектура компьютера». Изучение дисциплины является базой для дальнейшего освоения студентами курсов по выбору профессионального цикла, прохождения педагогической практики.

1.3 Дисциплина направлена на формирование следующих компетенций: УК-8, ОПК-4:

- УК-8. Способен создавать и поддерживать безопасные условия жизнедеятельности, в том числе при возникновении чрезвычайных ситуаций:

- УК-8.1 Оценивает факторы риска, умеет обеспечивать личную безопасность и безопасность окружающих.

- ОПК-4. Способен осуществлять духовно-нравственное воспитание обучающихся на основе базовых национальных ценностей:

- ОПК-4.2 Демонстрирует способность к формированию у обучающихся гражданской позиции, толерантности и навыков поведения в изменяющейся поликультурной среде, способности к труду и жизни в условиях современного мира, культуры здорового и безопасного образа жизни.

1.4 Перечень планируемых результатов обучения. В результате изучения дисциплины студент должен

- знать:

- положения основных нормативных документов, регламентирующих деятельность в области защиты информации;
- основные уязвимости, возникающие при защите компьютерных систем и факторы, влияющие на уровень защищенности;
- основные математические методы и принципы построения средств защиты информации;
- основные подходы к выявлению и предотвращению компьютерных атак;

- уметь:

- формулировать основные принципы защиты компьютерных систем;
- выявлять основные узлы компьютерных систем, подверженные атакам, и предъявлять методы для их защиты;
- получать качественные оценки защищенности компьютерных систем;

- владеть:

- базовыми программными методами защиты информации при работе с компьютерными системами и организационными мерами и приемами антивирусной защиты;
- навыками установки, настройки и использования средств защиты информации,
- приемами и программными средствами выявления компьютерных атак;
- навыками оценки уровня защищенности компьютерных систем.

1.5 Общая трудоемкость дисциплины «Методы и средства защиты информации» составляет 2 зачетные единицы (далее – ЗЕ) (72 часа):

№	Наименование раздела	Курс	Семестр	Кол-во часов	ЗЕ
1.	Методы и средства защиты информации	4	9	72	2

Программа предусматривает изучение материала на лекциях и практических занятиях. Предусмотрена самостоятельная работа студентов по темам и разделам. Проверка знаний осуществляется фронтально, индивидуально.

1.6 Объем дисциплины и виды учебной деятельности

Объем дисциплины и виды учебной деятельности (очная форма обучения)

Вид учебной работы	Всего часов	Семестр 9
Общая трудоемкость	72	72
Аудиторные занятия	36	36
Лекции	14	14
Практические занятия	22	22
Самостоятельная работа	36	36
Вид итогового контроля		зачёт

2 УЧЕБНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

2.1 Очная форма обучения

Учебно-тематический план

№	Наименование тем (разделов)	Всего часов	Аудиторные занятия		Самостоятельная работа
			Лекции	Практические занятия	
1.	Введение в защиту информации. Общая проблема информационной безопасности.	2	1		1
2.	Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах. Защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение)	2	1		1
3.	Правовое обеспечение информационной безопасности	4	1		3
4.	Организационное обеспечение информационной безопасности	2	1		1
5.	Технические средства обеспечения информационной безопасности	4	1		3
6.	Защита информации от несанкционированного доступа. Предотвращение несанкционированного доступа к компьютерным ресурсам и защи-	8	1	4	3

	та программных средств				
7.	Защита от компьютерных вирусов	6	1	2	3
8.	Математические и методические средства защиты. Криптографическое закрытие информации	8	1	4	3
9.	Уничтожение остаточных данных	6	1	2	3
10.	Защита от потери информации и отказов программно-аппаратных средств	4	1		3
11.	Компьютерные средства реализации защиты в информационных системах. Защита информационно-программного обеспечения на уровне операционных систем	8	1	4	3
12.	Защита информации на уровне систем управления базами данных	4	1		3
13.	Специфические особенности защиты информации в локальных и глобальных компьютерных сетях	10	1	6	3
14.	Программа информационной безопасности России и пути ее реализации. Современные средства защиты информации от НСД	4	1		3
	Зачёт				
ИТОГО		**72**	**14**	**22**	**36**

Интерактивное обучение по дисциплине

№	Наименование тем (разделов)	Вид занятия	Форма интерактивного занятия	Кол-во часов
1.	Организационное обеспечение информационной безопасности	Л	Лекция-дискуссия	1
2.	Программа информационной безопасности России и пути ее реализации. Современные средства защиты информации от НСД	Л	Лекция-дискуссия	1
3.	Математические и методические средства защиты. Криптографическое закрытие информации	ЛР	Работа в парах	4
4.	Защита от компьютерных вирусов	ЛР	Работа в парах	3
5.	Защита информации от несанкционированного доступа. Предотвращение несанкцио-	ЛР	Работа в парах	3

	нированного доступа к компьютерным ресурсам и защита программных средств			
ИТОГО				**12**

3 СОДЕРЖАНИЕ ТЕМ (РАЗДЕЛОВ)

Тема 1. Введение в информационную безопасность. Общая проблема информационной безопасности информационных систем.

Понятие национальной безопасности: виды безопасности: государственная, экономическая, общественная, военная, экологическая, информационная; роль и место системы обеспечения информационной безопасности (ИБ) в системе национальной безопасности РФ; доктрина ИБ, история проблемы ИБ, угрозы ИБ; методы и средства обеспечения ИБ; методологические и технологические основы комплексного обеспечения ИБ; модели, стратегии и системы обеспечения ИБ; методы управления, организации и обеспечения работ по обеспечению ИБ; обеспечение ИБ в нормальных и чрезвычайных ситуациях; проблемы информационной войны. Предмет защиты. Основные составляющие информационную безопасность.

Тема 2. Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах. Защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение).

Структура и принципы функционирования современных вычислительных систем. Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах. Базовые этапы построения системы комплексной защиты вычислительных систем. Анализ моделей нарушителя. Угрозы информационно-программному обеспечению вычислительных систем и их классификация. Функции системы защиты по предупреждению угроз и устранению последствий их реализации. Классификация способов и средств комплексной защиты информации. Классификация методов защиты информации с использованием программно-аппаратных средств вычислительной системы.

Организационная структура системы комплексной защиты информационно-программного обеспечения. Управление системой защиты. Функции ядра системы комплексной защиты. Многоуровневая структура системы защиты на основе программно-аппаратных средств вычислительной системы. Проектирование системы защиты.

Тема 3. Правовое обеспечение информационной безопасности.

Правовые и нормативные акты в области ИБ. Российское законодательство в области информационной безопасности, защиты государственной тайны и конфиденциальной информации; конституционные гарантии прав граждан на информацию и механизм их реализации; понятие и виды защищаемой информации по законодательству РФ; защита интеллектуальной собственности средствами патентного и авторского права; правовая регламентация охранной деятельности; международное законодательство в области защиты информации. Обзор зарубежного законодательства в области информационной безопасности.

Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт. Рекомендации Х.800. Стандарт «Критерии оценки безопасности информационных технологий». Руководящие документы Гостехкомиссии России.

Тема 4. Организационное обеспечение информационной безопасности.

Основные определения и критерии классификации угроз. Случайные угрозы. Преднамеренные угрозы. Основные угрозы целостности, доступности, конфиденциальности. Анализ и оценка угроз информационной безопасности объекта; оценка ущерба вслед-

ствие противоправного раскрытия информации ограниченного доступа и меры по его локализации; средства и методы физической защиты объектов; системы сигнализации, видеонаблюдения, контроля доступа; служба безопасности объекта; подбор, расстановка и работа с кадрами; организация и обеспечение режима секретности; организация пропускного и внутриобъектового режима; организация режима и охраны объектов в процессе транспортировки; защита информации при авариях, иных экстремальных ситуациях и в условиях чрезвычайного положения; технологические меры поддержания информационной безопасности объектов; обеспечение информационной безопасности объекта (учреждения, банка, промышленного предприятия) при осуществлении международного научно-технического и экономического сотрудничества.

Административный уровень информационной безопасности. Управление рисками. Основные понятия. Политика безопасности. Программа безопасности. Подготовительные этапы управления рисками. Основные этапы управления рисками.

Тема 5. Технические средства обеспечения информационной безопасности.

Общие вопросы организации противодействия технической разведке; основные организационные и технические мероприятия, используемые для противодействия технической разведке; методы и средства защиты режимных объектов от утечки конфиденциальной информации по техническим каналам; физические основы образования побочных электромагнитных излучений от технических средств; каналы утечки информации: электромагнитные, электрические (проводные), виброакустические; защита технических средств от утечки информации по этим каналам; нормы эффективности защиты; роль и место технического контроля эффективности защиты информации; нормы, руководящие документы по организации и ведению контроля; организационный и технический контроль; методы контроля; особенности контроля объектов в различных сферах; аппаратура контроля; взаимодействие контрольных органов с подразделениями контроля на местах; методологические основы автоматизации технического контроля; основные задачи технического контроля, требующие автоматизированного решения.

Тема 6. Защита информации от несанкционированного доступа. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств.

Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Основные этапы допуска к ресурсам вычислительной системы. Использование простого пароля. Использование динамически изменяющегося пароля. Взаимная проверка подлинности и другие случаи опознания. Способы разграничения доступа к компьютерным ресурсам. Разграничение доступа по спискам. Использование матрицы установления полномочий. Произвольное и принудительное управление доступом. Разграничение доступа по уровням секретности и категориям. Понятие меток безопасности. Управление метками безопасности. Парольное разграничение доступа и комбинированные методы. Особенности программной реализации контроля установленных полномочий. Защита программных средств от несанкционированного копирования, исследования и модификации. Привязка программ к среде функционирования. Защита программ от несанкционированного запуска.

Тема 7. Защита от компьютерных вирусов.

Вредоносное программное обеспечение. История появления компьютерных вирусов и факторы, влияющие на их распространение. Понятие компьютерного вируса. Основные этапы жизненного цикла вирусов. Объекты внедрения, режимы функционирования и специальные функции вирусов. Схемы заражения файлов. Схемы заражения загрузчиков. Способы маскировки, используемые вирусами. Классификация компьютерных вирусов. Общая организация защиты от компьютерных вирусов. Транзитный и динамиче-

ский режимы антивирусной защиты. Поиск вирусов по сигнатурам и обезвреживание обнаруженных вирусов. Углубленный анализ на наличие вирусов путем контроля эталонного состояния компьютерной системы. Защита от деструктивных действий и размножения вирусов. Использование средств аппаратного и программного контроля. Стратегия заблаговременной подготовки к эффективной ликвидации последствий вирусной эпидемии. Технология гарантированного восстановление вычислительной системы после заражения компьютерными вирусами.

Тема 8. Математические и методические средства защиты. Криптографическое закрытие информации.

Введение в криптографию. Представление защищаемой информации; угрозы безопасности информации; ценность информации; основные термины и понятия криптографии; открытые сообщения и их характеристики; модели открытых сообщений; исторический очерк развития криптографии; Типы криптографических систем. Простые методы шифрования: шифры подстановки и перестановки. Подстановки с переменным коэффициентом сдвига. Многослойные шифры. Использование псевдослучайных чисел для генерации ключей. Выбор порождающего числа и максимизация длины последовательности чисел ключа. Режимы шифрования. Особенности шифрования данных в режиме реального времени. Шифрование ключа при необходимости его хранения с зашифрованными данными. Скоростные и недетерминированные программные шифры. Основы скоростного шифрования. Внесение неопределенностей в процесс криптографических преобразований. Стандарты шифрования. Протоколы распределения ключей; протоколы установления подлинности; электронная цифровая подпись; Общая организация криптографической защиты информации. Использование общесистемных и специализированных программных средств для шифрования файлов и работы с секретными внешними носителями информации.

Тема 9. Уничтожение остаточных данных.

Введение в проблему. Виды остаточных данных. Способы защиты от несанкционированного использования остаточной информации. Использование специализированных программ по уничтожению остаточных данных. Специальные режимы и особенности шифрования данных в режиме реального времени с возможность мгновенного уничтожения данных. Использование общесистемных и специализированных программных средств для мгновенного уничтожения данных.

Тема 10. Защита от потери информации и отказов программно-аппаратных средств.

Основные способы защиты от потери информации и нарушений работоспособности вычислительных средств. Внесение функциональной и информационной избыточности. Способы резервировании информации. Правила обновления резервных данных. Методы сжатия информации. Архивация файловых данных. Особенности архивации на магнитные диски и магнитную ленту. Резервирование системных данных. Подготовка программных средств восстановления. Безопасная инсталляция программных средств. Общие сведения о нарушении доступа к дисковой и оперативной памяти. Технология восстановления дисковой и оперативной памяти. Диагностирование и устранение логических и физических дефектов магнитных дисков. Восстановление разметки дискеты и корневого каталога. Отмена результатов форматирования и восстановление поврежденных файлов данных. Защита файлов от удаления и восстановление удаленных файлов. Безопасное кэширование и дефрагментация дисковой памяти. Восстановление и оптимизация оперативной памяти компьютера. Ручное восстановление данных. Безопасное окончание работы на компьютере.

Тема 11. Защита информационно-программного обеспечения на уровне операционных систем.

Общие сведения о реализации защиты информационно-программного обеспечения в операционных системах. Классификация функций защиты по уровням безопасности, поддерживаемых операционной системой (ОС). Ядро безопасности ОС. Аппаратная основа реализации защиты на уровне ОС. Стандарты по оценке уровня безопасности ОС. Внесение функциональной и информационной избыточности ресурсов на уровне ОС. Основы надежного администрирования ОС. Используемые способы разграничения доступа к компьютерным ресурсам, а также службы регистрации и сигнализации. Средства ОС по диагностированию и локализации несанкционированного доступа к ресурсам ВС. Безопасные файловые системы современных ОС (HPFS, NTFS). Подсистемы безопасности современных ОС (Windows 95, Windows NT, UNIX), их недостатки и основные направления совершенствования. Парольная аутентификация. Одноразовые пароли. Идентификация/аутентификация с помощью биометрических данных. Ролевое управление доступом.

Тема 12. Защита информации на уровне систем управления базами данных.

Концептуальные вопросы построения уровней защиты систем управления базами данных (СУБД). Основные требования к подсистеме безопасности СУБД. Общие сведения о разграничении доступа к базам данных. Обязанности администратора по защите баз данных от несанкционированного доступа. Определение полномочий пользователей по доступу к базе данных. Использование матрицы полномочий для разграничения доступа к элементам баз данных. Мандатная система разграничения доступа. Защита данных при статистической обработке. Общее понятие о целостности базы данных. Типы ошибок, ведущих к нарушению целостности. Задание ограничений целостности. Транзакция и ее свойства. Восстановление базы данных. Особенности восстановления распределенной базы данных. Проблема непротиворечивости при параллельной обработке данных. Использование блокирования для управления параллельной обработкой. Метод независимого выполнения транзакций. Управление параллельными транзакциями на основе временных и версионных отметок. Метод обнаружения противоречивых записей журнала регистрации. Метод использования теста правильности. Разрешение тупиковых ситуаций. Инструментальные средства СУБД по обеспечению целостности баз данных.

Тема 13. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях.

Анализ структуры и принципов функционирования вычислительных сетей с позиции обеспечения информационной безопасности. Угрозы информационно-программному обеспечению, характерные только для распределенной вычислительной среды. Использование криптографических систем для защиты данных, циркулирующих в вычислительной сети. Особенности применения симметрических и асимметрических систем шифрования. Распределение ключей между узлами вычислительной сети. Выработка секретных ключей по Диффи-Хеллману. Распределение ключей с помощью асимметрических систем шифрования. Взаимное подтверждение подлинности при обмене сообщениями в сети. Поддержание целостности циркулирующих в сети сообщений. Формирование и проверка цифровой подписи. Защита от отрицания фактов отправки и приема сообщений. Защита от наблюдения за потоком сообщений (трафиком) в сети. Защита в Internet и Intranet. Основные понятия. Архитектурные аспекты. Использование межсетевых экранов (брандмауэров) для защиты информации в локальных вычислительных сетях. Классификация межсетевых экранов, их достоинства и недостатки. Ограничение доступа из локальной сети в Internet с помощью proxy-серверов. Безопасность JAVA-приложений. Анализ защищенности. Отказоустойчивость и зона риска. Обеспечение отказоустойчивости.

Тема 14. Программа информационной безопасности России и пути ее реализации. Современные средства защиты информации от НСД.

Методы и средства ограничения доступа к компонентам ЭВМ, надежность средств защиты компонент; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации, типовые решения в организации ключевых систем; защита программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий (РПВ), понятие изолированной программной среды, защита программ от изменения и контроль целостности; системные вопросы защиты программ и данных, основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности в типовых операционных системах, системах управления базами данных, вычислительных сетях.

4 МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ (УКАЗАНИЯ) ДЛЯ СТУДЕНТОВ ПО ИЗУЧЕНИЮ ДИСЦИПЛИНЫ

Самостоятельная работа студентов при изучении дисциплины «Методы и средства защиты информации» организуется с целью формирования общекультурных и профессиональных компетенций, понимаемых как способность применять знания, умения и личностные качества для успешной деятельности в определенной области, в том числе:

- формирования умений по поиску и использованию различных источников информации;
- качественного освоения и систематизации полученных теоретических знаний, их углубления и расширения по применению на уровне межпредметных связей;
- формирования умения применять полученные знания на практике;
- развития познавательных способностей студентов, формирования самостоятельности мышления;
- развития активности, творческой инициативы, самостоятельности, ответственности и организованности;
- формирования способностей к саморазвитию (самопознанию, самоопределению, самообразованию, самосовершенствованию, самореализации, саморегуляции);
- развития научно-исследовательских навыков;
- развития навыков межличностных отношений.

В ходе изучения дисциплины «Методы и средства защиты информации» предлагается выполнить различные виды самостоятельной работы:

- выполнение индивидуальных заданий на лабораторных занятиях;
- подготовка к аудиторным занятиям и выполнение заданий разного типа и уровня сложности; подготовка к проблемным лекциям, дискуссионным вопросам, коллоквиумам;
- изучение отдельных тем (вопросов) дисциплины в соответствии с учебно-тематическим планом, составление конспектов;
- составление логических и структурных схем;
- решение задач; выполнение самостоятельных и контрольных работ, выполнение домашних заданий, подготовка ответов на вопросы для самоконтроля, составление отчётов к лабораторным работам;
- выполнение проектных заданий (разработка проектов, моделей, программ, макетов и т.п.);
- выполнение мини-исследований;
- индивидуальные консультации, индивидуальные собеседования;

- подготовка ко всем видам контрольных испытаний, в том числе к текущему контролю успеваемости (в течение семестра), промежуточной аттестации (по окончании семестра);
- подготовка к итоговой государственной аттестации, в том числе подготовка к государственным экзаменам.

Требования к отчетам по лабораторным работам

1. Отчет оформляется в электронном виде в одном из форматов *.doc, *.docx, *.pdf.
2. Титульный лист должен содержать название работы, Ф.И.О. студента, номер варианта.
3. Отчет о выполнении заданий должен содержать: текст задания и результаты выполнения задания, а также анализ полученных результатов и выводы.

Самостоятельная работа студентов предполагает изучение теоретического материала по актуальным вопросам дисциплины и его обсуждение на семинарских занятиях, а также выполнение практических заданий.

Виды контроля. Текущий контроль за аудиторной и самостоятельной работой обучаемых осуществляется во время проведения аудиторных занятий посредством устного опроса, проведения контрольных работ или осуществления лекции в форме диалога. Итоговый контроль осуществляется после успешного прохождения студентами текущего и защиты индивидуальных заданий в виде зачета.

Методические рекомендации по проведению лабораторных работ. Лабораторный практикум затрагивает основные разделы дисциплины «Методы и средства защиты информации», имеют различный уровень сложности, и на их выполнение требуется различное количество часов. Лабораторный практикум предполагает самостоятельную работу студентов по освоению лекций и теоретического материала, вынесенного на самостоятельное изучение. Текущий контроль знаний осуществляется путем опроса студентов после выполнения работы.

Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине

№	Наименование раздела (темы)	Формы/виды самостоятельной работы	Количество часов, в соответствии с учебно-тематическим планом
1.	1. Введение в защиту информации. Общая проблема информационной безопасности.	Изучение основной и дополнительной литературы по теме лекции. Работа с ресурсами Интернет.	1
2.	2. Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах. Защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение)	Изучение основной и дополнительной литературы по теме лекции. Работа с ресурсами Интернет.	1

3.	3. Правовое обеспечение информационной безопасности	Изучение основной и дополнительной литературы по теме лекции. Работа с ресурсами Интернет.	3
4.	4. Организационное обеспечение информационной безопасности	Подготовка к лекции-дискуссии. Работа с конспектом и рекомендуемой литературой по теме лекции для систематизации учебного материала.	1
5.	5. Технические средства обеспечения информационной безопасности	Изучение основной и дополнительной литературы по теме лекции. Работа с ресурсами Интернет.	3
6.	6. Защита информации от несанкционированного доступа. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств	Выполнение лабораторной работы. Работа с конспектом и рекомендуемой литературой по теме лекции для систематизации учебного материала. Работа с ресурсами Интернет.	3
7.	7. Защита от компьютерных вирусов	Выполнение лабораторной работы. Работа с конспектом и рекомендуемой литературой по теме лекции для систематизации учебного материала. Работа с ресурсами Интернет.	3
8.	8. Математические и методические средства защиты. Криптографическое закрытие информации	Выполнение лабораторной работы. Работа с конспектом и рекомендуемой литературой по теме лекции для систематизации учебного материала. Работа с ресурсами Интернет.	3
9.	9. Уничтожение остаточных данных	Выполнение лабораторной работы. Работа с конспектом и рекомендуемой литературой по теме лекции для систематизации учебного материала. Работа с ресурсами Интернет.	3
10.	10. Защита от потери информации и отказов программно-аппаратных средств	Работа с конспектом и рекомендуемой литературой по теме лекции для систематизации учебного материала. Работа с ресурсами Интернет.	3
11.	11. Компьютерные средства реализации защиты в информационных системах. Защита информационно-программного обес-	Выполнение лабораторной работы. Работа с конспектом и рекомендуемой литературой по теме лекции для	3

	печения на уровне операционных систем	систематизации учебного материала. Работа с ресурсами Интернет.	
12.	12. Защита информации на уровне систем управления базами данных	Изучение основной и дополнительной литературы по теме лекции. Работа с ресурсами Интернет.	3
13.	13. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях	Выполнение лабораторной работы. Работа с конспектом и рекомендуемой литературой по теме лекции для систематизации учебного материала. Работа с ресурсами Интернет.	3
14.	14. Программа информационной безопасности России и пути ее реализации. Современные средства защиты информации от НСД	Подготовка к лекции-дискуссии. Работа с конспектом и рекомендуемой литературой по теме лекции для систематизации учебного материала.	3
	ИТОГО		**36**

5 ПРАКТИКУМ ПО ДИСЦИПЛИНЕ

Тема 1. Защита информации от несанкционированного доступа. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств.
Содержание. Оценочный расчет защищенности помещений от утечки речевых сообщений по акустическому каналу. Оценочный расчет защищенности помещений от утечки информации по электромагнитному каналу.

Тема 2. Математические и методические средства защиты. Криптографическое закрытие информации.
Содержание. Изучение традиционных симметричных криптосистем. Шифры перестановок. Изучение традиционных симметричных криптосистем Шифры замены.

Тема 3. Защита от компьютерных вирусов.
Содержание. Защита от компьютерных вирусов.

Тема 4. Компьютерные средства реализации защиты в информационных системах. Защита информационно-программного обеспечения на уровне операционных систем
Содержание. Защита информационно-программного обеспечения на уровне операционных систем.

Тема 5. Уничтожение остаточных данных.
Содержание. Уничтожение остаточных данных.

Тема 6. Специфические особенности защиты информации в локальных и глобальных компьютерных сетях.
Содержание. Защита информации в локальных и глобальных компьютерных сетях.

Литература:

1. Мельников, В.П. Информационная безопасность и защита информации [Текст] : учеб. пособие для студ. вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. – 4-е изд., стер. – М.: Академия, 2009. – 330, [1] с. – (Высшее профессиональное образование).
2. Расторгуев, С.П. Основы информационной безопасности [Текст] : учеб. пособие / С. П. Расторгуев. – 2-е изд., стер. – М.: Академия, 2009. – 186, [1] с. – (Высшее профессиональное образование).
3. Баранова, Е.К. Информационная безопасность и защита информации: учеб. пособие / Е. К. Баранова, А. В. Бабаш. – 2-е изд. – М.: РИОР: ИНФРА-М, 2014. – 254 с.
4. Молдовян, А. А. Криптография: учеб. пособие / А. А. Молдовян, Н. А. Молдовян, Б. Я. Советов. – СПб.: Лань, 2001. – 218 с. – (Учебники для вузов. Специальная литература).

6 ДИДАКТИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ КОНТРОЛЯ (САМОКОНТРОЛЯ) УСВОЕННОГО МАТЕРИАЛА

6.1 Оценочные средства, показатели и критерии оценивания компетенций

Индекс компетенции	Оценочное средство	Показатели оценивания	Критерии оценивания сформированности компетенций
УК-8 ОПК-4	Тест	Низкий (неудовлетворительно)	Количество правильных ответов на вопросы теста менее 60 %
		Пороговый (удовлетворительно)	Количество правильных ответов на вопросы теста от 61-75 %
		Базовый (хорошо)	Количество правильных ответов на вопросы теста от 76-84 %
		Высокий (отлично)	Количество правильных ответов на вопросы теста от 85-100 %
	Дискуссия	Низкий – 0 баллов (неудовлетворительно)	Не раскрыто основное содержание учебного материала; обнаружено незнание или непонимание большей или наиболее важной части учебного материала; допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов; не сформированы компетенции, умения и навыки публичной речи, аргументации, ведения дискуссии и полемики, критического восприятия информации
		Пороговый – 2 баллов (удовлетворительно)	Неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала; имелись затруднения или допущены

			ошибки в определении понятий, использовании терминологии, исправленные после нескольких наводящих вопросов; при неполном знании теоретического материала выявлена недостаточная сформированность компетенций, умений и навыков, студент не может применить теорию в новой ситуации.
		Базовый – 4 баллов (хорошо)	Ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков: в усвоении учебного материала допущены небольшие пробелы, не исказившие содержание ответа; допущены один – два недочета в формировании навыков публичной речи, аргументации, ведения дискуссии и полемики, критического восприятия информации.
		Высокий – 6 баллов (отлично)	Студент полно усвоил учебный материал; конкретными примерами, применять их в новой ситуации; высказывать свою точку зрения; продемонстрировано усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость компетенций, умений и навыков.
	Реферат	Низкий – до 60 баллов (неудовлетворительно)	Не раскрыто основное содержание учебного материала; обнаружено незнание или непонимание большей или наиболее важной части учебного материала; допущены ошибки в определении понятий, при использовании терминологии, которые не исправлены после нескольких наводящих вопросов; не сформированы компетенции, умения и навыки публичной речи, аргументации, ведения дискуссии и полемики, критического восприятия информации
		Пороговый – 61-75 баллов (удовлетворительно)	Неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала; имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, исправленные после нескольких наводящих вопросов; при неполном знании теоретического материала выявлена недостаточная сформированность компетенций, умений и навыков, студент не мо-

			жет применить теорию в новой ситуации.
		Базовый – 76-84 баллов (хорошо)	Ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков: в усвоении учебного материала допущены небольшие пробелы, не исказившие содержание ответа; допущены один – два недочета в формировании навыков публичной речи, аргументации, ведения дискуссии и полемики, критического восприятия информации.
		Высокий – 85-100 баллов (отлично)	Студент полно усвоил учебный материал; конкретными примерами, применять их в новой ситуации; высказывать свою точку зрения; продемонстрировано усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость компетенций, умений и навыков.
	Лабораторная работа	Низкий – до 60 баллов (неудовлетворительно)	Лабораторная работа студенту не засчитывается если студент: 1. допустил число ошибок и недочетов превосходящее норму, при которой пересекается пороговый показатель; 2. или если правильно выполнил менее половины работы.
		Пороговый – 61-75 баллов (удовлетворительно)	Если студент правильно выполнил не менее половины работы или допустил: 1. не более двух грубых ошибок; 2. или не более одной грубой и одной негрубой ошибки и одного недочета; 3. или не более двух-трех негрубых ошибок; 4. или одной негрубой ошибки и трех недочетов; 5. или при отсутствии ошибок, но при наличии четырех-пяти недочетов.
		Базовый – 76-84 баллов (хорошо)	Если студент выполнил работу полностью, но допустил в ней: 1. не более одной негрубой ошибки и одного недочета; 2. или не более двух недочетов.
		Высокий – 85-100 баллов (отлично)	Если студент: 1. выполнил работу без ошибок и недочетов; 2. допустил не более одного недочета.
	Самостоятельная работа	Низкий – до 60 баллов (неудовлетворительно)	Работа студента не засчитывается если: 1. студент обнаруживает неумение выполнять решения большей части задания, 2. допускает грубые ошибки в решении

			задач, беспорядочно и неуверенно излагает материал.
		Пороговый – 61-75 баллов (удовлетворительно)	Студент обнаруживает знание формул и понимание основных методов решения задач, но: 1. излагает решения неполно и допускает неточности в вычислениях; 2. не умеет рационально решать задачи.
		Базовый – 76-84 баллов (хорошо)	Студент выполняет работу полностью, обнаруживает понимание материала, но: 1. допускает некоторые вычислительные ошибки; 2. небрежно оформляет решения; 3. демонстрирует решения задач только в рамках алгоритмов, изученных на занятиях.
		Высокий – 85-100 баллов (отлично)	Студент получает высокий балл, если: 1. выполняет задание в полном объеме; 2. обнаруживает понимание материала; 3. использует рациональные способы решения задач; 4. демонстрирует умение пользоваться дополнительными источниками знаний.
	Контрольная работа	Низкий – до 60 баллов (неудовлетворительно)	Контрольная работа не засчитывается если студент: 1. допустил число ошибок и недочетов превосходящее норму, при которой пересекается пороговый показатель; 2. или если правильно выполнил менее половины работы.
		Пороговый – 61-75 баллов (удовлетворительно)	Если студент правильно выполнил не менее половины работы или допустил: 1. не более двух грубых ошибок; 2. или не более одной грубой и одной негрубой ошибки и одного недочета; 3. или не более двух-трех негрубых ошибок; 4. или одной негрубой ошибки и трех недочетов; 5. или при отсутствии ошибок, но при наличии четырех-пяти недочетов.
		Базовый – 76-84 баллов (хорошо)	Если студент выполнил работу полностью, но допустил в ней: 1. не более одной негрубой ошибки и одного недочета; 2. или не более двух недочетов.
		Высокий – 85-100 баллов (отлично)	Если студент: 1. выполнил работу без ошибок и недочетов; 2. допустил не более одного недочета.

6.2 Промежуточная аттестация студентов по дисциплине

Промежуточная аттестация является проверкой всех знаний, навыков и умений студентов, приобретённых в процессе изучения дисциплины. Формой промежуточной аттестации по дисциплине является зачёт.

Для оценивания результатов освоения дисциплины применяется следующие критерии оценивания.

Критерии оценивания устного ответа на зачете

Оценка «зачтено» выставляется студенту, если:

- прочно усвоил предусмотренный программный материал; вопросы раскрыты, изложены логично, без существенных ошибок;
- правильно, аргументировано ответил на все вопросы, показано умение иллюстрировать теоретические положения конкретными примерами;
- показал глубокие систематизированные знания, владеет приемами рассуждения и сопоставляет материал из разных источников: теорию связывает с практикой, другими темами данного курса, других изучаемых предметов;
- допустил незначительные ошибки.

Оценка «не зачтено» выставляется студенту, если:

- не раскрыл основное содержание учебного материала;
- показал незнание или непонимание большей, или наиболее важной части учебного материала;
- допустил ошибки в определении понятий, которые не исправил после нескольких наводящих вопросов;
- не может ответить на дополнительные вопросы, предложенные преподавателем или, в ответах на другие вопросы допустил существенные ошибки.

6.3 Типовые контрольные задания или иные материалы, необходимые для оценки результатов освоения дисциплины

Пример тестового задания

На выполнение заданий теста дается 20 минут.
Количество заданий – 12.
К каждому заданию даются возможные ответы, один из которых правильный.
За правильный ответ на вопрос – 1 балл.
Максимальное количество набранных баллов – 12.

Вариант 1

1. Меры информационной безопасности направлены на защиту от:
   a) нанесения неприемлемого ущерба
   b) нанесения любого ущерба
   c) подглядывания в замочную скважину
2. Что из перечисленного не относится к числу основных аспектов информационной безопасности?
   a) доступность
   b) целостность
   c) конфиденциальность
   d) правдивое отражение действительности

3. Затраты организаций на информационную безопасность:
   a) растут
   b) остаются на одном уровне
   c) снижаются

4. Что такое защита информации?
   a) защита от несанкционированного доступа к информации
   b) выпуск бронированных коробочек для дискет
   c) комплекс мероприятий, направленных на обеспечение информационной безопасности

5. Компьютерная преступность в мире:
   a) остается на одном уровне
   b) снижается
   c) растет

6. Основные угрозы доступности информации:
   a) непреднамеренные ошибки пользователей
   b) злонамеренное изменение данных
   c) хакерская атака
   d) отказ программного и аппаратно обеспечения
   e) разрушение или повреждение помещений
   f) перехват данных

7. Суть компрометации информации.
   a) внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации
   b) несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений
   c) внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений

8. Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, ...
   a) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой - ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды
   b) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации
   c) способна противостоять только информационным угрозам, как внешним так и внутренним
   d) способна противостоять только внешним информационным угрозам

9. Методы повышения достоверности входных данных.
   a) Замена процесса ввода значения процессом выбора значения из предлагаемого множества
   b) Отказ от использования данных
   c) Проведение комплекса регламентных работ
   d) Использование вместо ввода значения его считывание с машиночитаемого носителя

e) Введение избыточности в документ первоисточник
f) Многократный ввод данных и сличение введенных значений

10. Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ).
a) МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения
b) МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты
c) МЭ работают только на сетевом уровне, а СОВ – еще и на физическом

11. Сервисы безопасности:
a) идентификация и аутентификация
b) шифрование
c) инверсия паролей
d) контроль целостности
e) регулирование конфликтов
f) экранирование
g) обеспечение безопасного восстановления
h) кэширование записей

12. Под угрозой удаленного администрирования в компьютерной сети понимается угроза ...
a) несанкционированного управления удаленным компьютером
b) внедрения агрессивного программного кода в рамках активных объектов Web-страниц
c) перехвата или подмены данных на путях транспортировки
d) вмешательства в личную жизнь
e) поставки неприемлемого содержания

Перечень примерных вопросов к лекциям-дискуссиям

1. Что такое информация?
2. Конфиденциальность информации
3. Защита информации
4. Информационная инфраструктура
5. Угроза
6. Инцидент информационной безопасности
7. Информационная безопасность
8. Информационная безопасность автоматизированных систем
9. Государственная тайна
10. Компьютерная безопасность
11. Целостность информации

Примерные темы рефератов

1. Информационное право и информационная безопасность.
2. Концепция информационной безопасности.
3. Основы экономической безопасности предпринимательской деятельности.
4. Анализ законодательных актов об охране информационных ресурсов открытого доступа.
5. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.

6. Соотношение понятий: информационные ресурсы, информационные системы и информационная безопасность.

7. Информационная безопасность **(**по материалам зарубежных источников и литературы).

8. Правовые основы защиты конфиденциальной информации.

9. Экономические основы защиты конфиденциальной информации.

10. Организационные основы защиты конфиденциальной информации.

11. Структура, содержание и методика составления перечня сведений, относящихся к предпринимательской тайне.

12. Составление инструкции по обработке и хранению конфиденциальных документов.

13. Направления и методы защиты документов на бумажных носителях.

14. Направления и методы защиты машиночитаемых документов.

15. Архивное хранение конфиденциальных документов.

16. Направления и методы защиты аудио- и визуальных документов.

17. Порядок подбора персонала для работы с конфиденциальной информацией.

18. Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.

19. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.

20. Порядок проведения переговоров и совещаний по конфиденциальным вопросам.

21. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.

22. Порядок работы с посетителями фирмы, организационные и технические методы защиты секретов фирмы.

23. Порядок защиты информации в рекламной и выставочной деятельности.

24. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.

25. Анализ источников, каналов распространения и каналов утечки информации (на примере конкретной фирмы).

26. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.

27. Основы технологии обработки и хранения конфиденциальных документов (по зарубежной литературе).

28. Назначение, виды, структура и технология функционирования системы защиты информации.

29. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.

30. Аналитическая работа по выявлению каналов утечки информации фирмы.

31. Анализ функций секретаря-референта небольшой фирмы в области защиты информации.

32. Направления и методы защиты профессиональной тайны.

33. Направления и методы защиты служебной тайны.

34. Направления и методы защиты персональных данных о гражданах.

35. Методы защиты личной и семейной тайны.

36. Построение и функционирование защищенного документооборота.

37. Защита секретов в дореволюционной России.

38. Методика инструктирования и обучения персонала правилами защиты секретов фирмы.

Пример лабораторной работы

Исследование оптимальных кодов. Коды Шеннона-Фано и Хаффмена (6 часов)

Оптимальные коды применяются в тех случаях, когда символы алфавита встречаются в сообщениях с различной вероятностью. В этом случае применение оптимальных кодов позволяет минимизировать избыточность кода, а, следовательно, сократить время передачи сообщений. Код Шеннона-Фано и код Хаффмана относятся к множеству оптимальных кодов. Алгоритм Шеннона-Фано – один из первых алгоритмов сжатия, который впервые сформулировали американские учёные Шеннон и Фано. Данный метод сжатия имеет большое сходство с алгоритмом Хаффмана, который появился на несколько лет позже. Алгоритм использует коды переменной длины: символы, имеющие большую вероятность появления, кодируется кодом меньшей длины, символы с малой вероятностью появления – кодом большей длины. Рассмотрим каждый из алгоритмов в отдельности.

Алгоритм оптимального кодирования Шеннона-Фано:

1. Все символы алфавита упорядочиваются в порядке убывания вероятности их появления.
2. Кодируемые символы делятся на две равновероятные или приблизительно равновероятные подгруппы.
3. Каждому символу из верхней подгруппы присваивается код «0», а каждому символу из нижней подгруппы – код «1».
4. Каждая из подгрупп снова делится на две равновероятные или приблизительно равновероятные подгруппы. При этом каждому символу из верхней подгруппы присваивается код «0», а из нижней – «1».
5. Деление на подгруппы проводится до тех пор, пока в подгруппе не останется по одному символу.
6. Результирующие кодовые слова записываются слева направо по кодам подгрупп, соответствующих кодируемому символу.

Отметим, что рассмотренная методика построения оптимального кода имеет некоторую неоднозначность для случаев, когда невозможно разбить символы алфавита на подгруппы с равными вероятностями. В таких случаях для одного и того же распределения вероятностей появления символов алфавита могут быть получены коды различной длины. Этой неоднозначности можно избежать, если для построения эффективного кода использовать алгоритм кодирования Хаффмана.

Алгоритм оптимального кодирования Хаффмана:

1. Все символы алфавита упорядочиваются в порядке убывания их вероятностей появления.
2. Проводится «укрупнение» символов. Для этого два последних символа «укрупняются» в некоторый вспомогательный символ с вероятностью, которая равняется сумме вероятностей символов, которые были «укрупнены».
3. Образовавшаяся новая последовательность вновь сортируется в порядке убывания вероятностей с учетом вновь образованного за счет «укрупнения» символа.
4. Процедура повторяется до тех пор, пока не получится один «укрупненный» символ, вероятность которого равна 1.

Задание

1. Выбрать из своей фамилии имени и отчества первые десять букв. В результирующей последовательности каждая буква должна встречаться только один раз.
2. Составить таблицу, состоящую из двух столбцов. В первый столбец должна быть записана буква из последовательности, выбранной в п.1, во втором столбце – соответствующая вероятность появления символа. Вероятность последней, десятой буквы последовательности вычислить с помощью соотношения

$$P_{10} = 1 - \sum_{i=1}^{9} P_i \ .$$

Это делается для того, чтобы суммарная вероятность для группы из выбранных десяти символов алфавита равнялась 1.

3. Для последовательности символов из п.1. построить оптимальный код Шеннона-Фано.
4. Для последовательности символов из п.1. построить оптимальный код Хаффмана.
5. Рассчитать энтропию источника с помощью соотношения

$$H = -\sum_{i=1}^{10} P_i \cdot \log(P_i) \left[\frac{бит}{символ} \right].$$

6. Рассчитать среднее количество элементарных символов на один символ первичного алфавита с помощью соотношения

$$l_{ср} = \sum_{i=1}^{10} P_i \cdot l_i \left[\frac{бит}{символ} \right].$$

Расчеты выполнить отдельно для метода Шеннона-Фано $l_{ср}^{Ш-Ф}$ и отдельно для метода Хаффмана $l_{ср}^{X}$.

7. Рассчитать недогруженность по методу Шеннона-Фано и по методу Хаффмана, используя соотношения

$$\Delta D_{Ш-Ф} = l_{ср}^{Ш-Ф} - H \left[\frac{бит}{символ} \right] \text{ и } \Delta D_X = l_{ср}^{X} - H \left[\frac{бит}{символ} \right].$$

8. Рассчитать избыточность, которая показывает, сколько процентов букв может быть удалено из текста без утраты смысла сообщения, используя соотношения

$$D_{Ш-Ф} = \frac{\Delta D_{Ш-Ф}}{l_{ср}^{Ш-Ф}} \left[\frac{бит}{символ} \right] \text{ и } D_X = \frac{\Delta D_X}{l_{ср}^{X}} \left[\frac{бит}{символ} \right].$$

9. Сравнить полученные в п. 7–8 результаты для каждого метода и сделать выводы.

Пример контрольной работы

Задача 1. Программная реализация криптографических алгоритмов

Зашифровать фразу, которую образуют свои имя и фамилия симметричным методом по алгоритму двойных перестановок. Размер таблицы выбрать самостоятельно (в соответствии с суммой знаков в имени и фамилии, недостающее количество знаков до полного заполнения таблицы заполнить любыми знаками). Создать и представить исходную и преобразованные таблицы, полученную шифровку. Выполнить проверку, расшифровав полученное сообщение.

Задача 2. Анализ рисков информационной безопасности

Проанализировать и оценить риски информационной безопасности предприятия по своему варианту в соответствии с ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

1. Загрузите ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

2. Ознакомьтесь с Приложениями C, D и E ГОСТа.

3. Выберите три различных информационных актива организации (см. вариант).

4. Из Приложения D ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

5. Пользуясь Приложением C ГОСТа, напишите три угрозы, реализация которых возможна, пока в системе не устранены названные в пункте 4 уязвимости.

6. Пользуясь одним из методов (см. вариант), предложенных в Приложении E ГОСТа, произведите оценку рисков информационной безопасности.

7. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

№ варианта	Организация	Метод оценки риска (см. Приложение Е ГОСТа)
1	Банк	1
2	Поликлиника	2
3	Университет	3
4	Интернет-магазин	1
5	Туристическое агенство	2

Перечень примерных вопросов и заданий для *Самостоятельной работы*

1. Изложить принципы и направления комплексного подхода к обеспечению информационной безопасности предприятия.
2. Назвать основные положения концепции информационной безопасности предприятия.
3. Изложить содержание регламента обеспечения информационной безопасности предприятия.
4. Определить основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации.
5. Определить критерии ценности информационных ресурсов и длительности сохранения ими этой характеристики.
6. Проанализировать содержание понятия разрешительной системы доступа персонала к конфиденциальным сведениям фирмы.
7. Обосновать критерии выделения конфиденциальных документов из общего потока поступающих документов.
8. Обосновать состав показателей учетной карточки (по выбору преподавателя) и правила их заполнения.
9. Проанализировать особенности контроля за исполнением конфиденциальных документов, его организационное и технологическое отличие от контроля открытых документов.
10. Классифицировать состав бумажных и технических носителей информации, применяемых для составления деловой (управленческой) и технической конфиденциальной документации.
11. Проанализировать особенности текста конфиденциального документа.
12. Регламентировать в виде фрагмента инструкции порядок работы исполнителей с конфиденциальными документами.
13. Проанализировать пути использования существующих средств копирования и тиражирования документов для изготовления экземпляров и копий конфиденциальных документов.
14. Сформулировать возможности, трудности и направления использования электронной почты для передачи конфиденциальных документов.
15. Составить фрагмент номенклатуры дел, содержащих конфиденциальные документы.
16. Проанализировать задачи защиты информации, которые должны быть решены при формировании и оформлении дел с конфиденциальными документами.
17. Классифицировать способы и средства физического уничтожения документов, изготовленных на носителях различных типов.
18. Проанализировать пути поиска документов и дел, не обнаруженных при проверке их наличия, дать рекомендации, повышающие эффективность поиска и предотвращающие утрату документов и дел.

19. Составить и проанализировать технологическую схему (цепочку) приема (перевода) лиц на работу, связанную с владением конфиденциальной информацией.

20. Составить и проанализировать технологическую схему (цепочку) увольнения сотрудников, владеющих конфиденциальной информацией. .

21. Проанализировать виды угроз безопасности конфиденциальной информации фирмы при демонстрации на выставке новой продукции.

22. Составить схему каналов возможной утраты конфиденциальной информации, находящейся в компьютере, локальной сети, проанализировать степень опасности каждого канала.

23. Назвать основные элементы физической защиты территории и помещений предприятия.

24. Охарактеризовать способы и элементы программно-технической защиты информационных ресурсов.

25. Дать классификацию компьютерных вирусов.

26. Описать основные антивирусные программы.

27. Охарактеризовать основные способы криптографического преобразования данных.

Вопросы к зачету

1. Понятие ИБ. Основные составляющие ИБ и их роль при создании ИС.
2. Значение и роль ИБ в современном мире.
3. Угрозы ИБ (основные определения) и критерии классификации угроз.
4. Примеры угроз и рисков по всем основным составляющим (аспектам) ИБ.
5. Анализ угроз и рисков ИС с точки зрения ИБ.
6. Российское и международное законодательство в области защиты информации.
7. Стандарты и спецификации в области защиты информации, их основные положения и принципы построения.
8. «Оранжевая книга» как оценочный стандарт.
9. Критерии оценки безопасности информационных технологий
10. Основные механизмы и сервисы безопасности.
11. Сетевая безопасность, наиболее характерные угрозы для сетевых ИС, точки входа.
12. Административный уровень ИБ (основные понятия, политика безопасности).
13. Программа безопасности, синхронизация программы безопасности с жизненным циклом систем.
14. Управление рисками. Основные понятия, принципы, этапы.
15. Процедурный уровень ИБ, классификация мер этого уровня.
16. Принципы физической и архитектурной безопасности ИС. Иерархическая организация ИС.
17. Идентификация и аутентификация (способы, их достоинства и недостатки), управление доступом.
18. Управление доступом, технологии, принципы организации, типичные решения.
19. Технологии протоколирования и аудита. Принципы построения и задачи, зависимость от других средств ИБ.
20. Использование криптографических технологий в ИС.
21. Технические средства, обеспечивающие защиту информации, их классификация и назначение.
22. Реагирование на нарушение режима безопасности, процедуры плановых восстановительных работ.
23. Особенности современных информационных систем, существенные с точки зрения безопасности.
24. Ролевое управление доступом.

25. Активный и пассивный аудит.

7 ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ В ПРОЦЕССЕ ОБУЧЕНИЯ

Информационные технологии – обучение в электронной образовательной среде с целью расширения доступа к образовательным ресурсам, увеличения контактного взаимодействия с преподавателем, построения индивидуальных траекторий подготовки, объективного контроля и мониторинга знаний студентов.

В образовательном процессе по дисциплине используются следующие информационные технологии, являющиеся компонентами Электронной информационно-образовательной среды БГПУ:

- Официальный сайт БГПУ;
- Корпоративная сеть и корпоративная электронная почта БГПУ;
- Система электронного обучения ФГБОУ ВО «БГПУ»;
- Электронные библиотечные системы;
- Мультимедийное сопровождение лекций и практических занятий;
- Тренажеры, виртуальные среды.

8 ОСОБЕННОСТИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ ИНВАЛИДАМИ И ЛИЦАМИ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

При обучении лиц с ограниченными возможностями здоровья применяются адаптивные образовательные технологии в соответствии с условиями, изложенными в раздел «Особенности организации образовательного процесса по образовательным программам для инвалидов и лиц с ограниченными возможностями здоровья» основной образовательной программы (использование специальных учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь и т.п.) с учётом индивидуальных особенностей обучающихся.

9 СПИСОК ЛИТЕРАТУРЫ И ИНФОРМАЦИОННЫХ РЕСУРСОВ

9.1 Литература

1. Введение в криптографию : базовый курс для студ. математич. спец. вузов / ред. В. В. Ященко. - 3-е изд. - М. ; Харьков ; Минск; СПб. : Питер, 2001. - 287 с. (9 экз.)

2. Галатенко В.А. Основы информационной безопасности : курс лекций для студ.вузов,обучающихся по спец."Прикладная информатика" / Галатенко В.А. - М. : Интернет-Ун-т информационных технологий, 2003. - 277 с. (10 экз.)

3. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. – Москва : Издательство Юрайт, 2022. – 104 с. – (Высшее образование). – ISBN 978-5-534-14590-8. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/497002 (дата обращения: 10.10.2022).

4. Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие для студ. вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. – 4-е изд., стер. – М. : Академия, 2009. – 330 с. (6 экз.)

5. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. – Москва : Издательство Юрайт, 2022. – 309 с. – (Высшее

образование). – ISBN 978-5-534-04732-5. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/490019 (дата обращения: 10.10.2022).

6. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. – Москва : Издательство Юрайт, 2022. – 253 с. – (Высшее образование). – ISBN 978-5-534-13960-0. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/496741 (дата обращения: 10.10.2022).

7. Расторгуев, С.П. Основы информационной безопасности [Текст] : учеб. пособие / С. П. Расторгуев. – 2-е изд., стер. – М.: Академия, 2009. – 186, [1] с. – (Высшее профессиональное образование). (5 экз.)

8. Соболев, А. Н. Физические основы технических средств обеспечения информационной безопасности [Text] : учеб. пособие для студ. вузов / А. Н. Соболев. - М. : Гелиос АРВ, 2004. - 221 с. (16 экз.)

9.2 Базы данных и информационно-справочные системы

1. Онлайн-курсы от ведущих университетов и организаций - https://www.coursera.org
2. «Национальная платформа открытого образования» - https://openedu.ru
3. Федеральная университетская компьютерная сеть России - https://runnet.ru
4. Российская площадка массовых открытых онлайн-курсов (МООК) - https://universarium.org
5. Современная цифровая образовательная среда в Российской Федерации - https://online.edu.ru
6. Портал Электронная библиотека: диссертации - http://diss.rsl.ru
7. Портал научной электронной библиотеки - http://elibrary.ru/defaultx.asp
8. http://fstec.ru – официальный сайт Федеральная служба по техническому и экспортному контролю.
9. Сайт Российской академии наук. - Режим доступа: http://www.ras.ru
10. Сайт Государственного научно-исследовательского институт информационных технологий и телекоммуникаций. - Режим доступа: http://www.informika.ru
11. Сайт Президента РФ. - Режим доступа: http://www.president.kremlin.ru
12. Сайт Правительства РФ. - Режим доступа: www.government.ru
13. Сайт Министерства науки и высшего образования РФ. - Режим доступа: https://minobrnauki.gov.ru
14. Сайт Министерства просвещения РФ. - Режим доступа: https://edu.gov.ru
15. Сайт Федеральной службы государственной статистики РФ. - Режим доступа: www.gks.ru
16. Сайт Федеральной службы по интеллектуальной собственности, патентам и товарным знакам (Роспатента). - Режим доступа: http://www.fips.ru/rospatent/index.htm

9.3 Электронно-библиотечные ресурсы

1. Polpred.com Обзор СМИ/Справочник http://polpred.com/news
2. ЭБС «Лань» http://e.lanbook.com

10 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА

Для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используются аудитории, оснащённые учебной мебелью, аудиторной доской, компьютером(рами) с установленным лицензионным специализированным программным обеспечением, с доступом в электронно-библиотечную систему, электронную информационно-образовательную среду БГПУ и в сеть Интернет, мультимедийными

проекторами, экспозиционными экранами, учебно-наглядными пособиями (мультимедийные презентации и пр.).

Для проведения практических занятий также используются компьютерные классы физико-математического факультета, оснащённые учебной мебелью, аудиторной доской, компьютерами с установленным лицензионным программным обеспечением, с доступом в электронно-библиотечную систему, электронную информационно-образовательную среду БГПУ и в сеть Интернет, мультимедийными проекторами, экспозиционными экранами, учебно-наглядными пособиями (мультимедийные презентации и пр.).

Самостоятельная работа студентов организуется в аудиториях оснащенных компьютерной техникой и в залах доступа в локальную сеть БГПУ с выходом в электронную информационно-образовательную среду вуза и в сеть Интернет.

Лицензионное программное обеспечение: операционные системы семейства Windows, Linux; офисные программы Microsoft office, Libreoffice, OpenOffice;, DrWeb antivirus и т.д .

Разработчик: Матевосян А.С. – ст. преподаватель кафедры информатики и методики.

11 ЛИСТ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ

Утверждение изменений и дополнений в РПД для реализации в 2020/2021 уч. г.

РПД обсуждена и одобрена для реализации в 2020/2021 уч. г. на заседании кафедры информатики и методики преподавания информатики (протокол № 8 от «17» июня 2020 г.). В РПД внесены следующие изменения и дополнения:

№ изменения: 1 № страницы с изменением: на титульном листе	
Исключить:	Включить:
Текст: МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ	Текст: МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Утверждение изменений и дополнений в РПД для реализации в 2021/2022 уч. г.

РПД обсуждена и одобрена для реализации в 2021/2022 уч. г. без изменений на заседании кафедры (протокол № 7 от 24.04.2021 г.).

Утверждение изменений и дополнений в РПД для реализации в 2022/2023 уч. г.

РПД пересмотрена, обсуждена и одобрена для реализации в 2022/2023 учебном году на заседании кафедры информатики и методики преподавания информатики (протокол №1 от 21 сентября 2022 г.).

В рабочую программу внесены следующие изменения и дополнения:

№ изменения: 1 № страницы с изменением: 27	
В Раздел 9 внесены изменения в список литературы, в базы данных и информационно-справочные системы, в электронно-библиотечные ресурсы. Указаны ссылки, обеспечивающие доступ обучающимся к электронным учебным изданиям и электронным образовательным ресурсам с сайта ФГБОУ ВО «БГПУ».	