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
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки
09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

Профиль
«ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ»

Уровень высшего образования
БАКАЛАВРИАТ

Принята на заседании кафедры
кафедры информатики и МПИ
(протокол № 9 от «15» мая 2019 г.)

Благовещенск 2019

СОДЕРЖАНИЕ

1 ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1 Цель дисциплины: ознакомление с общей проблемой информационной безопасности информационных систем, организационными, техническими и другими методами и средствами защиты информации, с законодательством и стандартами в этой области, с современными криптосистемами, с компьютерными средствами реализации защиты в информационных системах, изучение методов идентификации пользователей, борьбы с вирусами; освоение фундаментальных знаний в области информационной безопасности и выработка практических навыков применения этих знаний.

1.2 Место дисциплины в структуре ООП: Дисциплина «Информационная безопасность» относится к дисциплинам обязательной части блока Б1 (Б1.О.25).

Содержание дисциплины «Информационная безопасность» входит в необходимый минимум профессиональных знаний. Преподавание дисциплины «Информационная безопасность» связано с другими дисциплинами профессионального цикла «Инфокоммуникационные системы и сети», «Архитектура информационных систем».

1.3 Дисциплина направлена на формирование следующих компетенций: ОПК-3, ПК-3:

- 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, индикаторами достижения которой является:

- ИД-1опк-з-знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
- ИД-2опк-з-уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
- ИД-3опк-з-иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно- исследовательской работе с учетом требований информационной безопасности.

- ПК-3. Способность обеспечивать требуемый качественный бесперебойный режим работы инфокоммуникационной системы, индикаторами достижения которой является:

- ИД-3пк-1-знает: Модели Института инженеров по электротехнике и радиоэлектронике (IEEE). Модель взаимодействия открытых систем (OSI) ISO. Основы системного администрирования. Средства защиты от несанкционированного доступа операционных систем и систем управления базами данных. Требования охраны труда при работе с сетевой аппаратурой, с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы.
- ИД-3пк-2-умеет: Идентифицировать права пользователей по доступу к программно-аппаратным средствам. Конфигурировать операционные системы, сетевые устройства. Параметризировать протоколы канального, сетевого и транспортного уровня модели взаимодействия открытых систем. Применять программно-аппаратные средства для диагностики отказов и ошибок сетевых устройств. Тестирование прототипа ИС на проверку корректности архитектурных решений.
- ИД-3пк-3-владеет навыком: Управления доступом к программно-аппаратным средствам. Контроля использования ресурсов сетевых устройств и ПО. Управления безопасностью сетевых устройств и ПО. Применять программно-аппаратные средства для диагностики отказов и ошибок ПО.

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

знать:

- знать правовые основы информационной безопасности и защиты информации;
- определение основных понятий защиты информации, типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду;
- способы шифрования компьютерных данных, стандарты, модели и методы шифрования;
- принципы криптографических преобразований, дискретное преобразование Фурье;
- типовые средства защиты информации и возможности их использования в реальных задачах создания и внедрения информационных систем;

уметь:

- уметь реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации;
- проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем;
- разрабатывать средства и системы защиты информации

владеть:

- методами защиты программ от вирусов;
- навыками аутентификации пользователей.

1.5 Общая трудоемкость дисциплины «Информационная безопасность» составляет 4 зачетные единицы (далее – ЗЕ) (144 часа).

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 7
Общая трудоемкость	144	144
Аудиторные занятия	54	54
Лекции	34	34
Лабораторные работы	20	20
Самостоятельная работа	54	54
Вид итогового контроля	36	экзамен

Объем дисциплины и виды учебной деятельности (заочная форма обучения)

Вид учебной работы	Всего часов	Семестр 9
Общая трудоемкость	144	144
Аудиторные занятия	16	16
Лекции	4	4
Лабораторные работы	12	12
Самостоятельная работа	119	119
Вид итогового контроля	9	экзамен

2 УЧЕБНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ

2.1 Очная форма обучения

Учебно-тематический план

№	Наименование тем (разделов)	Всего часов	Аудиторные занятия		Самостоятельная работа
			Лекции	Лабораторные работы	
1.	Введение в информационную безопасность. Общая проблема информационной безопасности информационных систем.	4	2		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)	8	4		4
3.	Правовое обеспечение информационной безопасности	6	2		4
4.	Организационное обеспечение информационной безопасности	4	2		2
5.	Технические средства обеспечения информационной безопасности	4	2		2
6.	Защита информации от несанкционированного доступа. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств	8	2		6
7.	Защита от компьютерных вирусов	6	2		4
8.	Математические и методические средства защиты. Криптографическое закрытие информации	20	4	10	6
9.	Уничтожение остаточных данных	8	2	2	4
10.	Защита от потери информации и отказов программно-аппаратных средств	6	2		4
11.	Компьютерные средства реализации защиты в информационных системах. Защита информационно-	10	2	4	4

	программного обеспечения на уровне операционных систем				
12.	Защита информации на уровне систем управления базами данных	6	2		4
13.	Специфические особенности защиты информации в локальных и глобальных компьютерных сетях	14	4	4	6
14.	Программа информационной безопасности России и пути ее реализации. Современные средства защиты информации от НСД	4	2		2
	Экзамен	36			
ИТОГО		**144**	**34**	**20**	**54**

Интерактивное обучение по дисциплине

№	Наименование тем (разделов)	Вид занятия	Форма интерактивного занятия	Кол-во часов
1.	Введение в информационную безопасность. Общая проблема информационной безопасности информационных систем.	Л	Лекция-дискуссия	10
2.	Защита информации от несанкционированного доступа. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств	ЛБ	Работа в парах	8
ИТОГО				**18**

2.2 Заочная форма обучения

Учебно-тематический план

№	Наименование тем (разделов)	Всего часов	Аудиторные занятия		Самостоятельная работа
			Лекции	Лабораторные работы	
1.	Введение в информационную безопасность. Общая проблема информационной безопасности информационных систем.	8,5	0,5		8
2.	Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах. Защита информации при реализации информационных процессов (ввод, вывод, передача, обработка, накопление, хранение)	11	1		10
3.	Правовое обеспечение информационной безопасности	8,5	0,5		8
4.	Организационное обеспечение информационной безопасности	8,5	0,5		8

5.	Технические средства обеспечения информационной безопасности	12,5	0,5		12
6.	Защита информации от несанкционированного доступа. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств	17,5	0,5	6	11
7.	Защита от компьютерных вирусов	8			8
8.	Математические и методические средства защиты. Криптографическое закрытие информации	13		6	7
9.	Уничтожение остаточных данных	8			8
10.	Защита от потери информации и отказов программно-аппаратных средств	7			7
11.	Компьютерные средства реализации защиты в информационных системах. Защита информационно-программного обеспечения на уровне операционных систем	8,5	0,5		8
12.	Защита информации на уровне систем управления базами данных	8			8
13.	Специфические особенности защиты информации в локальных и глобальных компьютерных сетях	8			8
14.	Программа информационной безопасности России и пути ее реализации. Современные средства защиты информации от НСД	8			8
	Экзамен	9			
ИТОГО		**144**	**4**	**12**	**119**

Интерактивное обучение по дисциплине

№	Наименование тем (разделов)	Вид занятия	Форма интерактивного занятия	Кол-во часов
1.	Введение в информационную безопасность. Общая проблема информационной безопасности информационных систем.	Л	Лекция-дискуссия	2
2.	Защита информации от несанкционированного доступа. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств	ЛБ	Работа в парах	4
	ИТОГО			**6**

3 СОДЕРЖАНИЕ ТЕМ (РАЗДЕЛОВ)

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.

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.

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.

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 вследствие 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.

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.

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.

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 динамический 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.

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.

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.

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. 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.

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.

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.

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. 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 Internetи 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.

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

Дисциплина изучается студентами в лекционных аудиториях и компьютерных классах.

Курс лекций строится на основе четких понятий и формулировок, так как только при таком подходе студенты приобретают культуру абстрактного мышления, необходимую для высококвалифицированного бакалавра в любой отрасли знаний.

Изложение материала должно быть по возможности простым и базироваться на уровне разумной строгости. Изложение теоретического материала дисциплины должно предшествовать лабораторным занятиям.

Внимательное слушание лекции, уяснение основного её содержания, краткая, но разборчивая запись лекции - условие успешной самостоятельной работы каждого студента. Поэтому студенты обязаны не только внимательно слушать преподавателя, но и конспектировать излагаемый им материал. При этом конспектирование материала представляет собой запись основных теоретических положений, рассуждений, излагаемых лектором. Нужно помнить, что конспектирование лекций дает студенту не только возможность пользоваться записями лекций при самостоятельной подготовке к занятиям и экзамену, но и глубже и основательней вникнуть в существо излагаемых в лекции вопросов, лучше усвоить и запомнить теоретический материал. Рекомендуется высказываемое лектором положение записывать своими словами. Перед записью надо постараться вначале понять смысл сказанного, необходимо стараться отделить главное от второстепенного и, прежде всего, записать основной материал. Качество записи лекции, конечно, во многом зависит от навыков конспектирующего, от его общей подготовки, от сообразительности, от умения излагать преподносимое преподавателем своими словами.

На отработку лабораторных заданий выделяется не менее 80% времени от общего времени на лабораторном занятии, остальные 20% времени выделяется на получение задания и отчётность за его выполнение перед преподавателем.

Отработка лабораторных заданий происходит следующим образом:

1) Преподаватель перед началом занятия выдаёт задания студентам в виде текстовых файлов, которые рекомендуется размещать на едином сетевом ресурсе в компьютерном классе или на информационном сервере;

2) Студент на экране компьютера внимательно изучает полученное задание, при необходимости задаёт вопросы и уточняет последовательность выполнения задания. При выполнении заданий лабораторных работ рекомендуется использовать учебно-методические материалы.

3) После выполнения задания студент сохраняет результаты работы в заданном месте на локальном диске ЭВМ рабочего места или на сетевом ресурсе.

4) Сдаёт выполненное задание преподавателю, для чего вызывает его, говорит, что закончил выполнение задания и поясняет последовательность работы. При необходимости задаёт вопросы и отвечает на дополнительные вопросы, возникающие у преподавателя, получает оценку.

При работе с литературой главное внимание следует уделять основной рекомендуемой литературе. Дополнительная литература предназначена для расширения кругозора студента и обеспечивает формирование дополнительных профессиональных знаний, умений и навыков.

Для успешного усвоения дисциплины необходима правильная организация самостоятельной работы студентов. Эта работа должна содержать:

- регулярную (еженедельную) проработку теоретического материала по конспектам лекций и учебникам;
- регулярную (еженедельную) подготовку к лабораторным занятиям, в том числе изучение описания лабораторных работ;
- выполнение контрольной и самостоятельной работ.

Особое внимание при организации самостоятельной работы следует уделить планированию подготовки. Планирование – важный фактор организации самостоятельной работы. Оно, во-первых, позволяет видеть перспективу работы, выявлять, распределять время и использовать его по своему усмотрению. Во-вторых, оно дисциплинирует, подчиняет поведение студента целям учебы. В связи с этим обязательно следует планировать свою самостоятельную работу в пределах недели. После того, как составлен

план, его следует строго выполнять. Правильно учитывая свое время и распределяя его в соответствии с расписанием занятий, студент при строгом соблюдении намеченного плана сможет выделить достаточное количество часов для самостоятельной работы.

В случае появления каких-либо вопросов следует обращаться к преподавателю в часы его консультаций. Критерием качества усвоения знаний могут служить аттестационные оценки по дисциплине и текущие оценки, выставляемые преподавателем в течение семестра.

Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине

№	Наименование раздела (темы)	Формы/виды самостоятельной работы	Количество часов, в соответствии с учебно-тематическим планом
1.	Введение в информационную безопасность. Общая проблема информационной безопасности информационных систем.	Подготовка к лекции-дискуссии. Работа с конспектом и рекомендуемой литературой по теме лекции для систематизации учебного материала.	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)	Подготовка к самостоятельной работе. Работа с конспектом и рекомендуемой литературой по теме лекции для систематизации учебного материала.	4
3.	Правовое обеспечение информационной безопасности	Написание реферата. Изучение основной и дополнительной литературы по теме лекции. Работа с ресурсами Интернет.	4
4.	Организационное обеспечение информационной безопасности	Изучение основной и дополнительной литературы по теме лекции. Работа с ресурсами Интернет.	2
5.	Технические средства обеспечения информационной безопасности	Изучение основной и дополнительной литературы по теме лекции. Работа с ресурсами Интернет.	2
6.	Защита информации от несанкционированного доступа. Предотвращение несанкционированного доступа к компьютерным ресурсам и защита программных средств	Подготовка к лабораторным работам. Работа с конспектом и рекомендуемой литературой по теме лекции для систематизации учебного материала.	6
7.	Защита от компьютерных вирусов	Выполнение контрольной работы. Изучение основной и дополнительной литературы по теме лекции.	4

8.	Математические и методические средства защиты. Криптографическое закрытие информации	Подготовка к лабораторным работам. Работа с конспектом и рекомендуемой литературой по теме лекции для систематизации учебного материала.	6
9.	Уничтожение остаточных данных	Изучение основной и дополнительной литературы по теме лекции. Работа с ресурсами Интернет.	4
10.	Защита от потери информации и отказов программно-аппаратных средств	Выполнение контрольной работы. Изучение основной и дополнительной литературы по теме лекции.	4
11.	Компьютерные средства реализации защиты в информационных системах. Защита информационно-программного обеспечения на уровне операционных систем	Изучение основной и дополнительной литературы по теме лекции. Работа с ресурсами Интернет.	4
12.	Защита информации на уровне систем управления базами данных	Изучение основной и дополнительной литературы по теме лекции. Работа с ресурсами Интернет.	4
13.	Специфические особенности защиты информации в локальных и глобальных компьютерных сетях	Подготовка к самостоятельной работе. Работа с конспектом и рекомендуемой литературой по теме лекции для систематизации учебного материала.	6
14.	Программа информационной безопасности России и пути ее реализации. Современные средства защиты информации от НСД	Подготовка к тесту. Работа с конспектом и рекомендуемой литературой по теме лекции для систематизации учебного материала.	2
	ИТОГО		**54**

5 ПРАКТИКУМ ПО ДИСЦИПЛИНЕ

Тема 9. Уничтожение остаточных данных

Содержание

Лабораторная работа №1. Программа безвозвратного удаления данных с носителей информации «Терьер». (2 часа).

Цели:

1. освоить работу с программой для безвозвратного удаления данных с носителей информации «Терьер»;
2. получить опыт работы с реализацией механизма безвозвратного удаления данных.

Задачи:

1. прочитать и выполнить инструктивную часть лабораторной работы;

2. продемонстрировать преподавателю результаты выполнения практического задания работы;
3. подготовить ответы на вопросы, приведённые в конце лабораторной работы;
4. ответить на вопросы преподавателя по лабораторной работе.

Тема 11. Компьютерные средства реализации защиты в информационных системах. Защита информационно-программного обеспечения на уровне операционных систем

Содержание

Лабораторная работа №2. Программа для контроля изменений объектов файловой системы «Фикс». (2 часа).

Цели:

1. освоить работу с программой для обнаружения изменений в объектах файловой системы;
2. получить опыт работы с реализацией механизма контроля целостности.

Задачи:

1. прочитать теоретические сведения;
2. прочитать и выполнить инструктивную часть лабораторной работы;
3. выполнить задания для самостоятельного выполнения в конце лабораторной работы;
4. продемонстрировать преподавателю результаты выполнения практического задания работы;
5. подготовить ответы на вопросы, приведённые в конце лабораторной работы;
6. ответить на вопросы преподавателя по лабораторной работе.

Лабораторная работа №3. Парольная защита (2 часа).

Цель:

познакомиться с механизмами парольной защиты.

Задания:

1. прочитать и выполнить инструкции к лабораторной работе;
2. подготовить ответы на вопросы, приведённые в конце работы;
3. продемонстрировать преподавателю выполненную практическую часть работы;
4. ответить на вопросы преподавателя.

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

Содержание

Лабораторная работа №4. Криптографическая защита данных на носителях информации **(2 часа).**

С точки зрения защиты конфиденциальной информации, стандартные способы хранения файлов на носителях информации имеют несколько уязвимостей. Как правило, файловая система хранит все файлы на физическом носителе в незашифрованном виде. Это означает, что при попадании жёстких дисков или других носителей в чужие руки вся информация с них может быть прочитана. Такие методы защиты, как пароли Windows и права на файлы, не остановят противника. Для борьбы с этим используется шифрование информации: в этом случае на физическом носителе данные хранятся в зашифрованном виде, что затрудняет доступ, даже если носитель попал в распоряжение противника.

Очень важен выбор программного обеспечения для шифрования: например, шифрование файлов, доступное в некоторых версиях Windows как стандартная функция операционной системы, является слабым и не сможет защитить от противника с профессиональными навыками. Однако, существует программное обеспечение, которое даёт качественную защиту даже против профессионального противника.

Одним из представителей такого программного обеспечения является программа VeraCrypt, которая относится к классу программ, предназначенных для криптографической защиты данных на компьютерных носителях информации. Работа VeraCrypt основывается на защищённых хранилищах, которые можно монтировать и использовать как обычные логические диски. Данные на таких дисках зашифрованы: все файлы, которые записываются на такой логический диск, шифруются при записи, и расшифровываются при чтении. Такая организация процессов шифрования и дешифровки называется шифрованием (дешифрованием) на лету. VeraCrypt позволяет создать шифрованное хранилище в виде отдельного файла или зашифровать жёсткий диск целиком или его раздел. В данной лабораторной работе рассматриваются оба варианта использования этой программы.

Лабораторная работа №5. Создание и использование сертификатов электронной цифровой подписи **(2 часа).**

Цель:

1. получить представления о механизмах создания и использования сертификатов электронной цифровой подписи;
2. получить опыт работы с сертификатами ЭЦП.

Задания:

1. прочитать и выполнить инструкцию к лабораторной работе;
2. подготовить ответы на вопросы, приведённые в конце работы;
3. продемонстрировать преподавателю выполненную практическую часть работы;
4. ответить на вопросы, заданные преподавателем.

Лабораторная работа №8. Создание и работа с зашифрованными хранилищами информации **(2 часа).**

Цель:

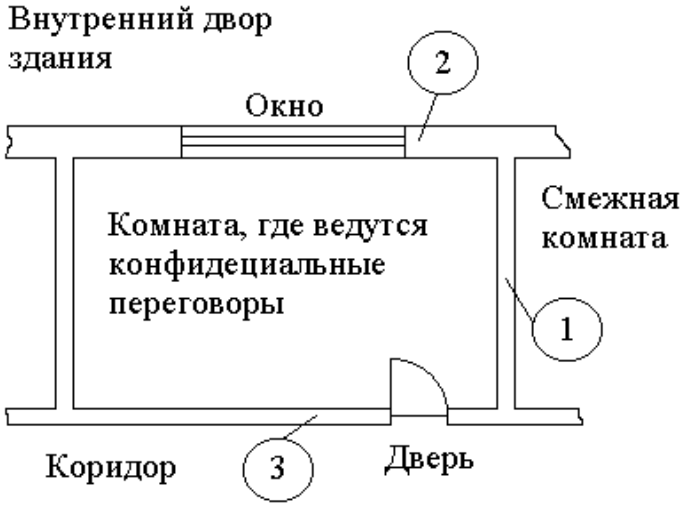
освоить простые криптографические средства защиты информации.

Задания:

1. прочитать и выполнить инструкцию к лабораторной работе;
2. подготовить ответы на вопросы, приведённые в конце работы;
3. продемонстрировать преподавателю выполненную практическую часть работы;
4. ответить на вопросы, заданные преподавателем.

Лабораторная работа №9. Создание и использование сертификатов электронной цифровой подписи **(2 часа).**

В соответствии со схемой рассчитать суммарную разборчивость формант в смежном помещении, коридоре и за наружной стеной. Сделать выводы о возможности или невозможности утечки звуковой информации.



Уровни интенсивности речи в октавных полосах берутся из табл. 1, для всех вариантов они одинаковы.

Ход выполнения лабораторной работы и ее результаты представьте в форме отчета.

Лабораторная работа №10. Создание и использование сертификатов электронной цифровой подписи **(2 часа).**

В соответствии со схемой (рис. 1) произвести расчеты защищенности помещения от утечки информации по электромагнитному каналу.

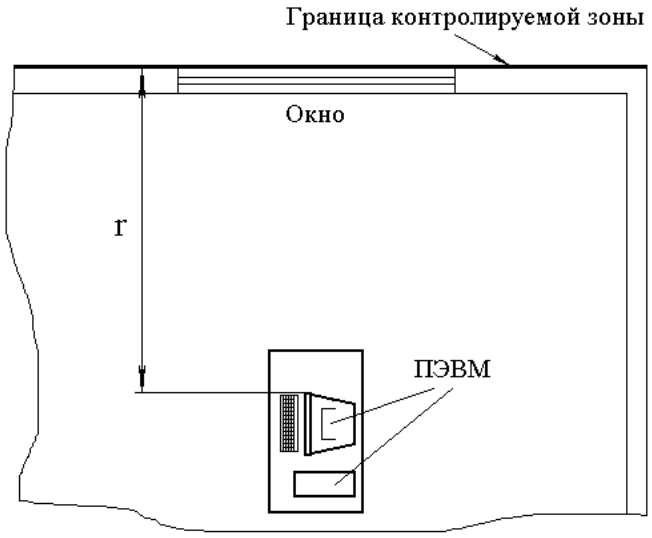


Рис. 1. Схема помещения для проведения расчетов

Среднеквадратические значения напряженности поля $\mathbf{E}_a$ атмосферных помех не рассчитывать, а считать одинаковыми для всех вариантов и равными:

	100 МГц	500 МГц	1000 МГц
$\mathbf{E}_a$, мкВ/м ($\mathbf{T}_a$=293°K, $f_{экв}$=40 МГц)	0,346	1,738	3,467

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

Содержание

Лабораторная работа №6. Построение VPN-сети с подключением по логину и паролю **(2 часа).**

Задания

Ознакомиться с описаниями технологии VPN и программного продукта SoftEther VPN.

Создать сеть из виртуальных машин, имеющую приведённую ниже конфигурацию.

Установить и настроить SoftEther VPN Server на серверной машине.

Установить и настроить SoftEther VPN Client на клиентских машинах.

Проверить работоспособность сети предложенными способами.

Общие сведения

VPN

Virtual Private Network — виртуальная частная сеть – это набор технологий, позволяющих построить логическую сеть поверх другой сети, например, Интернета. Такая логическая сеть может состоять из двух и более узлов, может быть одноразовой, то есть устанавливается для проведения только одного единственного сеанса работы, так и существовать на постоянной основе.

У сетей VPN есть два основных назначения: 1) построение локальной сети (соответственно организация совместной работы и распределение ресурсов машин, как правило, не находящихся физически в одной локальной сети), 2) организация защищённого обмена информацией между узлами, составляющими такую сеть. VPN часто применяются компаниями, для организации защищённого удалённого доступа сотрудников локальным сетям предприятия в случае удалённой работы, для объединения локальных сетей филиалов, находящихся на больших расстояниях друг от друга, в единую сеть компании, и для обмена особо важными данными, которые нельзя передавать по незащищённым каналам связи в открытом виде.

VPN не является единственным средством защиты передаваемых данных, но во многих случаях сеть VPN оказывается наиболее оптимальным решением, и часто — единственно верным.

Идея VPN состоит в том, что связь осуществляется по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), а уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений).

VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть.

Сеть VPN может быть построена как на основе специального оборудования, например маршрутизаторов компании Cisco, так и на основе специального программного обеспечения или комбинированного варианта.

Лабораторная работа №7. Построение VPN с подключением узлов к сети по сертификату **(2 часа).**

Задания

1. прочитайте материал раздела «Общие сведения»;
2. выполните подготовку к выполнению практической части лабораторной работы;

3. выполните установите соединение между клиентами и сервером через механизм аутентификации по сертификатам;
4. заблокируйте возможность подключения клиентов по одному из сертификатов;
5. установите механизм аутентификации сервера клиентом;
6. проверьте работоспособность сети.

Рекомендуются к прочтению следующие статьи:

1. LinuxFormat: «Электронные подписи и цифровые сертификаты. Часть 1.» http://wiki.linuxformat.ru/wiki/LXF93:Электронные_подписи
2. LinuxFormat: «Электронные подписи и цифровые сертификаты. Часть 2.» http://wiki.linuxformat.ru/wiki/LXF94:Электронные_подписи
3. OpenOffice Org: «Полезности: Как создать цифровую подпись в документе Ооо» https://wiki.openoffice.org/wiki/OOo_Полезности:_Как_создать_цифровую_подпись_в_документе_OOo#.D0.92.D0.B0.D1.80.D0.B8.D0.B0.D0.BD.D1.82_2._.D0.A1.D0.B0.D0.BC.D0.BE.D0.BF.D0.BE.D0.B4.D0.BF.D0.B8.D1.81.D0.B0.D0.BD.D0.BD.D1.8B.0.B9_.D1.81.D0.B5.D1.80.D1.82.D0.B8.D1.84.D0.B8.D0.BA.D0.B0.D1.82.

А также статьи из Wikipedia:

1. https://ru.wikipedia.org/wiki/Цифровой_сертификат
2. https://ru.wikipedia.org/wiki/Центр_сертификации
3. https://ru.wikipedia.org/wiki/Сертификат_открытого_ключа
4. https://ru.wikipedia.org/wiki/Электронная_подпись
5. https://ru.wikipedia.org/wiki/Инфраструктура_открытых_ключей

6 ДИДАКТИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ КОНТРОЛЯ (САМОКОНТРОЛЯ) УСВОЕННОГО МАТЕРИАЛА

6.1 Оценочные средства, показатели и критерии оценивания компетенций

Индекс компе-тенции	Оценочное средство	Показатели оценивания	Критерии оценивания сформированности компетенций

ОПК-3, ПК-3	Собеседование	Низкий (неудовлетворительно)	Студент отвечает неправильно, нечетко и неубедительно, дает неверные формулировки, в ответе отсутствует какое-либо представление о вопросе
		Пороговый (удовлетворительно)	Студент отвечает неконкретно, слабо аргументировано и не убедительно, хотя и имеется какое-то представление о вопросе
		Базовый (хорошо)	Студент отвечает в целом правильно, но недостаточно полно, четко и убедительно
		Высокий (отлично)	Ставится, если продемонстрированы знание вопроса и самостоятельность мышления, ответ соответствует требованиям правильности, полноты и аргументированности.
ОПК-3, ПК-3	Разноуровневые задачи и задания	Низкий (неудовлетворительно)	Ответ студенту не зачитывается если: • Задание выполнено менее, чем на половину; • Студент обнаруживает незнание большей части соответствующего материала, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно излагает материал.
		Пороговый (удовлетворительно)	Задание выполнено более, чем на половину. Студент обнаруживает знание и понимание основных положений задания, но: • Излагает материал неполно и допускает неточности в определении понятий; • Не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; • Излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.
		Базовый (хорошо)	Задание в основном выполнено. Ответы правильные, но: • В ответе допущены малозначительные ошибки и недостаточно полно раскрыто содержание вопроса; • Не приведены иллюстрирующие примеры, недостаточно чётко выражено обобщающие мнение студента; • Допущено 1-2 недочета в последовательности и языковом оформлении излагаемого.

		Высокий (отлично)	Задание выполнено в максимальном объеме. Ответы полные и правильные. • Студент полно излагает материал, дает правильное определение основных понятий; • Обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры; • Излагает материал последовательно и правильно с точки зрения норм литературного языка.
		Базовый (хорошо)	Задание в основном выполнено: • Студент твердо усвоил тему, грамотно и по существу излагает ее, опираясь на знания основной литературы; • Не допускает существенных неточностей; • Увязывает усвоенные знания с практической деятельностью; • Аргументирует научные положения; • Делает выводы и обобщения; • Владеет системой основных понятий.
		Высокий (отлично)	Задание выполнено в максимальном объеме. • Студент глубоко и всесторонне усвоил проблему; • Уверенно, логично, последовательно и грамотно его излагает; • Опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью; • Умело обосновывает и аргументирует выдвигаемые им идеи; • Делает выводы и обобщения; • Свободно владеет понятиями.

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 экзамен.

Для оценивания результатов освоения дисциплины применяется следующие критерии оценивания.

Критерии оценивания устного ответа на экзамене

Оценка 5 (отлично) ставится, если:

полно раскрыто содержание вопросов в объеме программы и рекомендованной ли-

тературы; четко и правильно даны определения и раскрыто содержание концептуальных понятий, закономерностей, корректно использованы научные термины; для доказательства использованы различные теоретические знания, выводы из наблюдений и опытов; ответ самостоятельный, исчерпывающий, без наводящих дополнительных вопросов, с опорой на знания, приобретенные в процессе специализации по выбранному направлению информатики.

Оценка 4 (хорошо) ставится, если:

раскрыто основное содержание вопросов; в основном правильно даны определения понятий и использованы научные термины; ответ самостоятельный; определения понятий неполные, допущены нарушения последовательности изложения, небольшие неточности при использовании научных терминов или в выводах и обобщениях, исправляемые по дополнительным вопросам экзаменаторов.

Оценка 3 (удовлетворительно) ставится, если:

усвоено основное содержание учебного материала, но изложено фрагментарно, не всегда последовательно; определение понятий недостаточно четкое; не использованы в качестве доказательства выводы из наблюдений и опытов или допущены ошибки при их изложении; допущены ошибки и неточности в использовании научной терминологии, определении понятий.

Оценка 2 (неудовлетворительно) ставится, если:

ответ неправильный, не раскрыто основное содержание программного материала; не даны ответы на вспомогательные вопросы экзаменаторов; допущены грубые ошибки в определении понятий, при использовании терминологии.

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

Перечень примерных вопросов к экзамену

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

Для обеспечения учебного процесса необходимо:

1) использование лекционной и лабораторной систем обучения, учебников, технических и визуальных средств обучения;
2) внутренняя локальная сеть БГПУ;
3) текстовый процессор Microsoft OfficeWord;
4) электронные таблицы Microsoft OfficeExcel;
5) системы программирования (C++, Java, Delphi, Pascal);
6) использование интернет-ресурсов для организации самостоятельной работы 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. Брэгг, Р. Безопасность сетей. Полное руководство / Р. Брэгг, М. Родс-Оусли, К. Страссберг. – М.: ЭКОМ: Бином. Лаборатория Знаний, 2011. – 911 с.(1)

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493262 (дата обращения: 13.10.2022).

3. 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: 13.10.2022).

Дополнительная

1. Торстейнсон, П. Криптография и безопасность в технологии .NET / П. Торстейнсон, Г. А. Ганеш; пер. с англ. В.Д. Хорева; под ред. С.М. Молявко. – М.: Бином. Лаборатория Знаний, 2007. – 479 с.(1)

2. Черемушкин, А.В. Криптографические протоколы. Основные свойства и уязвимости: учеб.пособие для студ. вузов / А.В. Черемушкин. – М.: Академия, 2009. – 271 с.(2)

3. Бармен, С. Разработка правил информационной безопасности.: Пер. с англ. / С. Бармен.– М.: Издательский дом «Вильямс», 2002. – 208 с.

4. Герасименко, В.А. Новые направления применения криптографических методов защиты информации. / В.А.Герасименко, А.А.Скворцов, И.Е. Харитонов. – М.: Радио и связь, 1989. – 360 с.

5. Защита программного обеспечения / Д. Гроувер – М.: Мир, 1992. – 280 с.

6. Зима, В.М. Безопасность глобальных сетевых технологий. / В.М. Зима, А.А. Молдовян, Н.А. Молдовян. - СПб: БХВ-Петербург. - 2000. – 368 с.

7. Петраков А.В. Защита и охрана личности, собственности, информации. – М.: Радио и связь, 1997. – 320 с.

8. Петренко, С.А. Аудит безопасности Intranet/ С.А.Петренко, А.А. Петренко. – М.: ДМК Пресс, 2002. – 416 с.

9. Советов, Б.Я. Введение в теорию защиты информации. / Б.Я. Советов, В.М. Зима, А.А. Молдовян. – СПб, Издательский центр СПбГЭТУ, 2001.

10. Спесивцев, А.В. Защита информации в персональных ЭВМ. / А.В. Спесивцев. – М.: Радио и связь, 1992. – 190 с.

11. Столлингс, В. Криптография и защита сетей: принципы и практика. Пер. с англ. / В. Столлингс. – М.: Изд. дом «Вильямс», 2001. – 672 с.

12. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Брюс Шнайер. – М.: Издательство ТРИУМФ, 2002 –816 с.

13. Аверченков, В.И. Методы и средства инженерно-технической защиты информации [Электронный ресурс] : учебное пособие / В.И. Аверченков, М.Ю. Рытов, А.В. Ку-

выклин [и др.]. — Электрон. дан. — М. : ФЛИНТА, 2011. — 187 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=60717 — Загл. с экрана.

14. Аникин, Д.В. Информационная безопасность и защита информации [Электронный ресурс] : . — Электрон. дан. — СПб. : ИЭО СПбУУиЭ (Институт электронного обучения Санкт-Петербургского университета управления и экономики), 2011. — 269 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=63950 — Загл. с экрана.

9.2 Базы данных и информационно-справочные системы

1. Федеральный портал «Российское образование» - http://www.edu.ru.
2. Информационная система «Единое окно доступа к образовательным ресурсам» - *http://www.window.edu.ru.*
3. Федеральный центр информационно-образовательных ресурсов - http://fcior.edu.ru.
4. Федеральный портал «Информационно-коммуникационные технологии в образовании» - *http://www.ict.edu.ru.*
5. Российский портал открытого образования - http://www.openet.ru/University.nsf/
6. Федеральная университетская компьютерная сеть России - http://www.runnet.ru/res.
7. Глобальная сеть дистанционного образования - *http://www.cito.ru/gdenet.*
8. Портал бесплатного дистанционного образования - www.anriintern.com
9. Портал научной электронной библиотеки - http://elibrary.ru/defaultx.asp.
10. Информационная система «Единое окно доступа к образовательным ресурсам». - Режим доступа: http://www.window.edu.ru/

Нормативные документы

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.
2. ГОСТ 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
3. Руководящий документ Гостехкомиссии России. Термины и определения в области защиты от НСД к информации. М.: ГТК РФ, 1992.
4. Руководящий документ Гостехкомиссии России. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. М.: ГТК РФ, 1992.
5. Руководящий документ Гостехкомиссии России. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. М.:ГТК РФ, 1992.
6. Руководящий документ Гостехкомиссии России. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. М.: ГТК РФ, 1992.
7. http://www.intuit.ru
8. http://www.citforum.ru

9.3 Электронно-библиотечные ресурсы

1. ЭБС «Юрайт». - Режим доступа: https://urait.ru
2. Полпред (обзор СМИ). - Режим доступа: https://polpred.com/news

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 с установленным лицензионным специализированным программным обеспечением, с выходом в электронно-библиотечную систему и электронную информационно-образовательную среду БГПУ, мультимедийными проекторами, экспозиционными экранами, учебно-наглядными пособиями (мультимедийные презентации).

Самостоятельная работа студентов организуется в аудиториях оснащенных компьютерной техникой с выходом в электронную информационно-образовательную среду вуза, в специализированных лабораториях по дисциплине, а также в залах доступа в локальную сеть БГПУ, в лаборатории психолого-педагогических исследований и др.

Для обеспечения учебного процесса необходимо:

- лекционная аудитория с мультимедиа-проектором;
- компьютерный класс с выходом в Интернет и внутреннюю сеть БГПУ;
- офисные программы: MS Office Word, MS Office Excel;
- системы программирования (C++, Java, Delphi, Pascal);
- браузеры.

Используемое программное обеспечение: Microsoft®WINEDUperDVC AllLng Upgrade/SoftwareAssurancePack Academic OLV 1License LevelE Platform 1Year; Microsoft®OfficeProPlusEducation AllLng License/SoftwareAssurancePack Academic OLV 1License LevelE Platform 1Year; Dr.Web Security Suite; Java Runtime Environment; Calculate Linux.

Разработчик: Серов М.А., кандидат технических наук

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: Титульный лист	
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. на заседании кафедры информатики и методики преподавания информатики (протокол № 7 от «21» апреля 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: 2 № страницы с изменением: 24-25	
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».	

Утверждение изменений и дополнений в РПД для реализации в 2023/2024 уч. г.

РПД пересмотрена, обсуждена и одобрена для реализации в 2023/2024 учебном году на заседании кафедры информатики и методики преподавания информатики (протокол № 9 от 26 июня 2023 г.).

Утверждение изменений и дополнений в РПД для реализации в 2024/2025 уч. г.

РПД пересмотрена, обсуждена и одобрена для реализации в 2024/2024 учебном году на заседании кафедры информатики и методики преподавания информатики (протокол № 9 от 26 июня 2024 г.).