Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Амурский государственный университет»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ Н.В.Савина
«29» 06 2018 г.

РАБОЧАЯ ПРОГРАММА

Защита информации в операционных системах

Направление подготовки 09.03.02 Информационные системы и технологии

Направленность (профиль) образовательной программы «Безопасность информационных систем»

Квалификация выпускника бакалавр

Программа подготовки академический бакалавриат

Год набора 2018

Форма обучения очная

Курс 3 Семестр 6

Экзамен 6 (27 акад. час.)

Лекции 36 (акад. час.)

Лабораторные занятия 36 (акад. час.)

Самостоятельная работа 81 (акад. час.)

Общая трудоемкость дисциплины 180 (акад. час.), 5 (з.е.)

Составители Фомин Д.В., ассистент; Сычёв М.С., к.т.н.

Факультет математики и информатики
Кафедра информационных и управляющих систем

2018г.

Рабочая программа составлена на основании Федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.02 «Информационные системы и технологии», утвержденного приказом Министерства образования и науки 12.03.2015 г., № 219

Рабочая программа обсуждена на заседании кафедры информационных и управляющих систем

«_15_» _____05_____201_8_г., протокол №_9_

Заведующий кафедрой _____ А.В. Бушманов
подпись И.О.Ф.

Рабочая программа одобрена на заседании УМС направления подготовки 09.03.02 «Информационные системы и технологии»

«_29_» _____05_____201_8_г., протокол №9_

Председатель _____ А. В. Бушманов
подпись И.О.Ф.

СОГЛАСОВАНО
Начальник учебно-методического управления _____ Н.А. Чалкина
(подпись)
«_29_» _____05_____20_18_ г.

СОГЛАСОВАНО
Заведующий выпускающей кафедрой _____ А. В. Бушманов
(подпись)
«_15_» _____05_____20_18__ г.

СОГЛАСОВАНО
Директор научной библиотеки _____ Л.А. Проказина
(подпись)
«_29_» _____05_____20_18_ г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины:

- расширение, углубление и развитие знаний и навыков из области информационной безопасности и защиты информации, приобретение знаний и навыков в области задач, механизмов, способов и средств защиты информации в контексте операционных систем.

Задачи дисциплины:

- развитие системы знаний и навыков общей теории информационной безопасности и защиты информации;
- формирование комплексных знаний об угрозах информационной безопасности в контексте операционных систем;
- формирование комплексных знаний о механизмах защиты информации, применяемых в операционных системах;
- формирование комплексных знаний и практических навыков решения задач защиты информации в операционных системах.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Защита информации в операционных системах» входит в вариативную часть блока базовых дисциплин учебного плана по направлению подготовки 09.03.02 «Информационные системы и технологии».

Для успешного освоения данной дисциплины необходимы знания, умения и навыки, приобретенные в результате освоения дисциплин учебного плана по направлению подготовки 09.03.02 «Информационные системы и технологии»: «Информационные технологии», «Информатика», «Архитектура информационных систем», «Операционные системы», «Инфокоммуникационные системы и сети».

На компетенциях, формируемых дисциплиной «Защита информации в операционных системах» базируются производственная практика и преддипломная практика, а также подготовка и защита выпускной квалификационной работы.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Изучение дисциплины обеспечивает овладение следующими компетенциями:

– понимание сущности и значения информации в развитии современного информационного общества, соблюдение основных требований к информационной безопасности, в том числе защите государственной тайны (ОПК-4);

– способность выбирать и оценивать способ реализации информационных систем и устройств (программно-, аппаратно- или программно-аппаратно-) для решения поставленной задачи (ОПК-6);

– способностью оценивать надежность и качество функционирования объекта проектирования (ПК-6);

– способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации (ДПК-1).

В результате освоения обучающийся должен демонстрировать следующие результаты образования:

1) Знать: основные виды и источники угроз информационной безопасности; основные виды ресурсов компьютера; основные подходы и методы защиты информации, применяемые в операционных системах; основные механизмы, реализующие данные подходы, и алгоритмы их работы; область применения, сильные и слабые стороны основных методов защиты информации; основные программные и программно-аппаратные средства, реализующие данные методы и механизмы.

2) Уметь: определять групп класса безопасности автоматизированных систем и средств вычислительной техники; выделять компьютерные ресурсы, требующие защиты; выбирать совокупность методов и механизмов, обеспечивающую требуемый уровень за-

щиты; выбирать, устанавливать, настраивать и обслуживать программные и программно-аппаратные средства, реализующие необходимые компоненты системы защиты информации.

3) Владеть: основными методами, способами и средствами оценки, обеспечения и повышения уровня защищённости информации и компьютерных ресурсов.

4. МАТРИЦА КОМПЕТЕНЦИЙ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

Темы (разделы) дисциплины	Компетенции			
	ОПК-4	ОПК-6	ПК-6	ДПК-1
Введение	+			+
Управление доступом	+	+	+	+
Идентификация и аутентификация	+	+	+	+
Журнализация и аудит	+	+	+	+
Замкнутая программная среда и контроль потоков информации	+		+	+
Контроль целостности	+	+	+	+
Резервное копирование	+	+	+	+
Типовая модель угроз безопасности в ОС	+		+	
Вредоносное программное обеспечение и способы борьбы с ним	+	+		+
Классы защищённости СВТ	+		+	
Классы защищённости АС	+		+	+

5.СТРУКТУРА ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины составляет 5 зачетные единицы, 180 академических часов.

№ п/п	Тема (раздел) дисциплины	Семестр	Неделя семестра	Виды контактной работы, включая самостоятельную работу студентов и трудоемкость (в акад. часах)			Формы текущего контроля успеваемости Форма промежуточной аттестации
				Лек.	Лаб.	Сам.	
1	2	3	4	5	6	7	8
1	Введение	6	1	2		5	Опрос
2	Управление доступом	6	2-3	4	4	7	Опрос, выполнение и защита лабораторной работы.
3	Идентификация и аутентификация	6	4-5	4	4	7	Опрос, выполнение и защита лабораторной работы.
4	Журнализация и аудит	6	6-7	4	4	7	Опрос, выполнение и защита лабораторной работы.
5	Замкнутая программная среда и контроль потоков информации	6	8-9	4	4	7	Опрос, выполнение и защита лабораторной работы.
6	Контроль целостности	6	10-11	4	4	7	Опрос, выполнение и защита лабораторной работы.
7	Резервное копирование	6	12	2	4	7	Опрос, выполнение и защита лабораторной работы.
8	Типовая модель угроз безопасности в ОС	6	13	2	4	7	Опрос, выполнение и защита лабораторной работы.

1	2	3	4	5	6	7	8
9	Вредоносное программное обеспечение и способы борьбы с ним	6	14	2	4	9	Опрос, выполнение и защита лабораторной работы.
10	Классы защищённости СВТ	6	15-16	4	2	9	Опрос, выполнение и защита лабораторной работы.
11	Классы защищённости АС	6	17-18	4	2	9	Опрос, выполнение и защита лабораторной работы.
Итого:			**1-18**	**36**	**36**	**81**	**экзамен (27 акад. час.)**

6. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1 Лекции

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)
1	2	3
1	Введение	Понятия информационной безопасности и защиты информации. Основные и дополнительные аспекты информационной безопасности. Угрозы информационной безопасности. Источники угроз. Классификации угроз. Виды компьютерных ресурсов. Группы мер защиты информации. Меры программно-технического уровня.
2	Управление доступом	Понятие доступа. Виды доступа. Задача управления доступом. Модели, механизмы, подходы разграничения доступа. Понятия объекта, субъекта, ресурса.
3	Идентификация и аутентификация	Понятия идентификации и аутентификации. Задача идентификации и аутентификации пользователя. Типы систем по отношению к процедуре идентификации-аутентификации. Факторы идентификации-аутентификации. Способы и механизмы организации процедур идентификации и аутентификации, их сильные и слабые места, области применения. Современные средства идентификации и аутентификации.
4	Журнализация и аудит	Понятия журнализации, аудита в узком смысле, аудита в широком смысле. Предназначение журнализации и аудита. Способы накопления, хранения и обработки регистрационной информации. Правила протоколирования. Активный и пассивный аудит. Рекомендации по проведению аудита. Системы автоматизированного аудита. Аудит в реальном времени. Системы обнаружения вторжений. Аудит в широком смысле: назначение, виды, общий алгоритм проведения.
5	Замкнутая программная среда и контроль потоков информации	Понятия замкнутой программной среды и контроля потоков информации. Назначение ЗПС. Способы организации работы механизма ЗПС. Способы настройки систем, реализующих замкнутую программную среду. Сильные и слабые стороны механизма ЗПС. Задача контроля потоков информации. Способы реализации механизма КПИ. Сильные и слабые стороны механизма КПИ.

1	2	3
6	Контроль целостности	Понятие контроля целостности. Назначение КЦ. Способы реализации идеи контроля целостности. Контрольная сумма. Сильные и слабые стороны различных способов организации контроля целостности. Связь контроля целостности с механизмом ЗПС.
7	Резервное копирование	Понятие резервного копирования. Назначение резервного копирования. Понятия носителя информации, плана резервного копирования. Схемы ротации резервных копий. Сильные и слабые стороны механизма резервного копирования. Рекомендации по организации и использованию резервного копирования.
8	Типовая модель угроз безопасности в ОС	Основные руководящие документы ФСТЭК России, их роль и назначение. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Модель угроз безопасности в ОС.
9	Вредоносное программное обеспечение и способы борьбы с ним	Понятие вредоносного ПО. Классификация вредоносного программного обеспечения. Программное обеспечение двойного назначения. Средства и методы противодействия угрозам, реализуемым с помощью вредоносного и потенциально опасного программного обеспечения. Антивирусы, сканеры, брандмауэры, мониторы процессов. Применение рассмотренных механизмов защиты информации для противодействия угрозам информационной безопасности, реализуемым с помощью вредоносного и потенциально опасного программного обеспечения.
10	Классы защищённости СВТ	Понятие средств вычислительной техники. Руководящий документ ФСТЭК России РД 1992.03.30-2. Группы и классы защищённости СВТ.
11	Классы защищённости АС	Понятие автоматизированных систем. Руководящий документ ФСТЭК России РД 1992.03.30-1. Группы и классы защищённости АС. Соотношение классов защищённости АС и СВТ с уровнем конфиденциальности обрабатываемой в них информации.

6.2. Лабораторные работы.

Тема 1. Система разграничения доступа в ОС Microsoft Windows.

Определение привилегий субъектов. Определение прав доступа субъектов и групп субъектов к объектам файловой системы и другим ресурсам компьютера.

Тема 2. Система идентификации и аутентификации в Windows.

Управление учётными записями. Настройка параметров идентификации и аутентификации пользователей.

Тема 3. Системные журналы ОС Windows.

Просмотр журнала. Фильтрация и поиск. Экспорт записей. Просмотр детализированной информации. Настройка параметров протоколирования.

Тема 4. Реализация механизмов ЗПС и КПИ в ОС Windows.

Определение потоков информации. Определение способов их контроля и блокировки. Использование встроенных средств ОС Windows для реализации КПИ. Использование встроенных средств ОС Windows для реализации механизма ЗПС.

Тема 5. Контроль целостности.

Определение объектов для механизма контроля целостности. Определение регламента работы механизма КЦ. Применение сторонних средств контроля целостности объектов ФС и реестра ОС Microsoft Window. Применение утилит для контроля целостности отдельных объектов ФС.

Тема 6. Резервное копирование.

Определение объектов для механизма резервного копирования. Определение регламента создания резервных копий. Применение встроенных средств резервного копирования ОС Microsoft Window. Восстановление данных из резервных копий.

Тема 7. Типовая модель угроз локальной операционной системы.

Рассмотрение компьютера с ОС Windows с точки зрения типовой модели угроз. Определение средств и способов защиты от них.

Тема 8. Шпионское и потенциально опасное программное обеспечение.

Знакомство с возможностями шпионского и потенциально опасного программного обеспечения. Сравнительный анализ программ данного класса.

Тема 9. Способы обнаружения и противодействия шпионскому и потенциально опасному программному обеспечению.

Признаки появления и работы на компьютере шпионского и потенциально опасного программного обеспечения. Способы предотвращения проникновения на компьютер шпионского и потенциально опасного программного обеспечения. Инструментальные средства обнаружения и противодействия шпионскому и потенциально опасному программному обеспечению (антивирусы, сканеры, брандмауэры, системы контроля целостности, журнализации, мониторы процессов).

Тема 10. Анализ СВТ и АС на соответствие заявленному уровню защищённости информации.

Анализ СВТ и АС по критериям рабочих документов ФСТЭК. Определение соответствия уровня защищённости СВТ и АС заявленному. Определение способов достижения соответствия СВТ и АС требованиям заявленного класса защищённости информации.

7. САМОСТОЯТЕЛЬНАЯ РАБОТА

№ п/п	Наименование темы (раздела)	Форма (вид) самостоятельной работы	Трудоёмкость в академических часах
1	2	3	4
1	Введение	Работа с лекционным материалом. Подготовка к опросу.	5
2	Управление доступом	Работа с лекционным материалом. Подготовка к опросу. Подготовка к лабораторным работам. Выполнение и защита лабораторной работы.	7
3	Идентификация и аутентификация	Работа с лекционным материалом. Подготовка к опросу. Подготовка к лабораторным работам. Выполнение и защита лабораторной работы.	7
4	Журнализация и аудит	Работа с лекционным материалом. Подготовка к опросу. Подготовка к лабораторным работам. Выполнение и защита лабораторной работы.	7
5	Замкнутая программная среда и контроль потоков информации	Работа с лекционным материалом. Подготовка к опросу. Подготовка к лабораторным работам. Выполнение и защита лабораторной работы.	7
6	Контроль целостности	Работа с лекционным материалом. Подготовка к опросу. Подготовка к лабораторным работам. Выполнение и защита лабораторной работы.	7

1	2	3	4
7	Резервное копирование	Работа с лекционным материалом. Подготовка к опросу. Подготовка к лабораторным работам. Выполнение и защита лабораторной работы.	7
8	Типовая модель угроз безопасности в ОС	Работа с лекционным материалом. Подготовка к опросу. Подготовка к лабораторным работам. Выполнение и защита лабораторной работы.	7
9	Вредоносное программное обеспечение и способы борьбы с ним	Работа с лекционным материалом. Подготовка к опросу. Подготовка к лабораторным работам. Выполнение и защита лабораторной работы.	9
10	Классы защищённости СВТ	Работа с лекционным материалом. Подготовка к опросу. Подготовка к лабораторным работам. Выполнение и защита лабораторной работы.	9
11	Классы защищённости АС	Работа с лекционным материалом. Подготовка к опросу. Подготовка к лабораторным работам. Выполнение и защита лабораторной работы.	9
	Всего		81

Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю):

1. Защита информации в операционных системах: сб. учеб.-метод. материалов для направления подготовки 09.03.02 /АмГУ, ФМиИ; сост.: Фомин Д.В., Сычев М.С. . – Благовещенск: Изд-во Амур. гос. ун-та, 2018. – 100 с. Режим доступа: http://irbis.amursu.ru/DigitalLibrary/AmurSU_Edition/10363.pdf.

Самостоятельная работа студентов состоит из аудиторной и внеаудиторной работы по изучению теоретического материала и выполнению заданий и расчетов. Целью выполнения заданий и расчетов является развитие и закрепление навыков решения прикладных задач.

Внеаудиторная работа студентов представлена

– подготовкой к лекциям и лабораторным занятиям;

– поиском теоретического и иллюстративного материала в сети Интернет.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе подготовки по дисциплине используется совокупность методов и средств обучения, позволяющих осуществлять целенаправленное методическое руководство учебно-познавательной деятельностью бакалавров, в том числе на основе интеграции информационных и традиционных педагогических технологий.

При реализации настоящей рабочей программы предусматриваются интерактивные и активные формы проведения занятий, дискуссии по темам исследования и поставленным научным проблемам.

Методы и формы организации обучения

ФОО / Методы	Лекц.	Лаб. зан.	СРС
1	2	3	4
IT-методы	+	+	+
Работа в команде		+	
Case-study		+	+
Игра			
Обучение на основе опыта		+	

1	2	3	4
Опережающая самостоятельная работа	+	+	+
Проектный метод		+	
Поисковый метод			+
Исследовательский метод		+	
Другие методы			

9. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания, типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков, характеризующих этапы формирования компетенций, а так же методические материалы, определяющие процедуры оценивания знаний, умений и навыков отражаются в фонде оценочных средств по данной дисциплине.

Текущий контроль по дисциплине осуществляется в следующих формах:

– устный опрос на проверку теоретических знаний, самостоятельная работа на проверку теоретических знаний.

Устный опрос проводится в течение 20 минут с целью закрепления теоретического материала, проверка вопросов самостоятельного изучения.

Вопросы к экзамену

1. Понятия информационной безопасности и защиты информации, угрозы, злоумышленника.
2. Основные аспекты ИБ.
3. Дополнительные аспекты ИБ
4. Угрозы ИБ
5. Система управления доступом: понятие, назначение, понятия объекта, субъекта.
6. Система управления доступом: понятие ресурса, виды ресурсов, виды доступа
7. Система управления доступом: модели разграничения доступа
8. Идентификация и аутентификация: понятия идентификации и аутентификации, назначение, роль в обеспечении ИБ.
9. Идентификация и аутентификация: факторы идентификации и аутентификации, идентификация основанная на знаниях пользователя.
10. Идентификация и аутентификация: факторы идентификации и аутентификации, идентификация основанная на предмете, которым владеет пользователь.
11. Идентификация и аутентификация: факторы идентификации и аутентификации, идентификация основанная на неотъемлемой части пользователя.
12. Журнализация: понятие, назначение, роль в обеспечении ИБ
13. Журнализация: способы организации протоколирования, основные принципы журнализации.
14. Аудит в узком смысле: понятие, назначение, роль в обеспечении ИБ
15. Аудит в узком смысле: связь с журнализацией, активный и пассивный аудит.
16. Аудит в широком смысле: понятие, назначение, роль в обеспечении ИБ, виды.
17. Контроль целостности: понятие, назначение, роль в обеспечении ИБ.
18. Контроль целостности: способы организации КЦ.
19. Контроль целостности: объекты КЦ, правила применения КЦ, источники угроз целостности информации.
20. Замкнутая программная среда: понятие, назначение, роль в обеспечении ИБ.
21. Замкнутая программная среда: объекты ЗПС, связь ЗПС с КЦ.

22. Замкнутая программная среда: способы настройки.
23. Контроль потоков информации: понятие, назначение, роль в обеспечении ИБ.
24. Контроль потоков информации: организация, связь с другими механизмами обеспечения ИБ.
25. Резервное копирование: понятие, назначение, роль в обеспечении ИБ, основные принципы.
26. Резервное копирование: создание протокола резервного копирования, способы организации ротации копий.
27. Вредоносное и шпионское программное обеспечение: понятия, реализуемые угрозы, способы противодействия и защиты.
28. Сетевой экран: понятие, назначение, роль в обеспечении ИБ.
29. Сетевой экран: виды, общий принцип работы.
30. Классы защищённости АС: понятие, группы, основные черты.
31. Классы защищённости СВТ: понятие, группы, основные черты.
32. Модель защиты системы не подключённой к сетям обмена информацией.

10.УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

а) основная литература

1. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Издательство Юрайт, 2018. — 321 с. — (Серия : Университеты России). — ISBN 978-5-534-00258-4. — Режим доступа: https://biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7 (ЭБС Юрайт);

2. Фомин Д.В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства [Электронный ресурс] : учебно-методическое пособие / Д.В. Фомин. — Электрон. текстовые данные. — Саратов: Вузовское образование, 2018. — 218 c. — 978-5-4487-0297-6. — Режим доступа: http://www.iprbookshop.ru/77317.html

б) дополнительная литература:

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — М. : Издательство Юрайт, 2018. — 312 с. — (Серия : Специалист). — ISBN 978-5-9916-9043-0. — Режим доступа: https://biblio-online.ru/book/E458AFCD-826E-4A1F-9BAB-68BB83EA616F (ЭБС Юрайт);

2. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 c.— Режим доступа: http://www.iprbookshop.ru/33430.— ЭБС «IPRbooks», по паролю;

3. Качановский Ю.П. Основные технические, программные и организационные меры защиты информации при работе с компьютерными системами [Электронный ресурс]: методические указания к проведению лабораторной работы по курсу «Информатика»/ Качановский Ю.П., Широков А.С.— Электрон. текстовые данные.— Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2014.— 24 c.— Режим доступа: http://www.iprbookshop.ru/55120.— ЭБС «IPRbooks», по паролю;

4. Защита информации в операционных системах: сб. учеб.-метод. материалов для направления подготовки 09.03.02 /АмГУ, ФМиИ; сост.: Фомин Д.В., Сычев М.С. . – Благовещенск: Изд-во Амур. гос. ун-та, 2018. – 100 с. Режим доступа: http://irbis.amursu.ru/DigitalLibrary/AmurSU_Edition/10363.pdf

в) нормативные источники

1. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информа-

ции [Электронный ресурс]: Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. №1 /. — Электрон. текстовые данные.— 1992.— Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g;

2. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации [Электронный ресурс]: Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. №2 /. — Электрон. текстовые данные.— 1992.— Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2;

3. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) [Электронный ресурс]: ФСТЭК России, 2008 год /.— Электрон. текстовые данные.— 2008.— Режим доступа: http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god.

г) программное обеспечение и Интернет-ресурсы

Перечень программного обеспечения:

№	**Перечень программного обеспечения (обеспеченного лицензией)**	**Реквизиты подтверждающих документов**
1	Операционная система MS Windows 7 Pro	DreamSpark Premium Electronic Software Delivery (3 years) договору – Сублицензионный договор №Tr000074357/KHB 17 от 01 марта 2016 года
2	MS office 2010 standard	Лицензия Microsoft office 2010 Standard RUS OLM ML Academic 50, договор №492 от 28 июня 2012 года
3	Kaspersky Endpoint Security 2010	Лицензия (Стандартный Russian Edition. 250-499 Node 1 year Educational Renewal License) по договору №129по/16 от 25 апреля 2016 года

Перечень Интернет-ресурсов

№	**Наименование ресурса**	**Краткая характеристика**
1	www.amursu.ru	Сайт ФГБОУ ВПО АмГУ
2	Электронная библиотечная система www.iprbookshop.ru	ЭБС IPRbooks — научно-образовательный ресурс для решения задач обучения в России и за рубежом. Уникальная платформа ЭБС IPRbooks в полном объеме соответствует требованиям законодательства РФ в сфере образования.
3	ЭБС ЮРАЙТ https://www.biblio-online.ru/	Фонд электронной библиотеки составляет более 4000 наименований и постоянно пополняется новинками, в большинстве своем это учебники и учебные пособия для всех уровней профессионального образования от ведущих научных школ с соблюдением требований новых ФГОСов.
4	Научная электронная библиотека www.elibrary.ru	Научная электронная библиотека eLIBRARY.RU. На платформе eLIBRARY.RU доступны электронные версии более 1400 российских научно- технических журналов, в том числе более 500 журналов в открытом доступе.

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Освоение материала учебной дисциплины обучающимся происходит посредством аудиторной работы на лекциях и лабораторных занятиях, а также в ходе самостоятельной работы обучающегося.

Количество лекционных и лабораторных занятий по каждой теме определяется учебным планом с учетом объема изучаемого материала.

Лекция является основной формой учебной работы в вузе, она является наиболее важным средством теоретической подготовки студентов. Поэтому следует внимательно слушать лекцию, следуя за ходом мысли автора и обязательно вести ее конспект. Добросовестные, старательные записи лекций способствуют более глубокому пониманию и осмыслению материала. Не следует отчаиваться, если конспекты первых лекций окажутся не совсем удачными. Студент должен постепенно овладевать техникой записи лекций.

Не надо стремиться к дословной, стенографической записи, записи все подряд. Это механический подход к слушанию лекции. Он отвлекает внимание на технику записи, а содержание лекции остается вне его пределов. Такая запись оказывается практически непригодной для использования. Главное – понять смысл сказанного, выделить главное, зафиксировать его в конспекте, а затем – те аргументы и факты, раскрывающие, доказывающие это главное. Надо следить за интонацией лектора. Как правило, преподаватель акцентирует внимание студентов на главном, выделяет важнейшие положения, выводы, произнося их громче и медленнее обычного. Обратите внимание на обязательность соблюдения таких правил записи лекций: отдельная тетрадь, чистота, аккуратность, наличие полей для дополнений и справок, нужный интервал между строчками (не мельчите, не уплотняйте записи). Хорошо выработать у себя систему сокращений слов, терминов, подчеркивать выводы, определения. Ни в коем случае нельзя делать «сплошных» записей, в которых трудно затем разобраться самому, а каждый раздел или новую мысль лектора начинать с новой строки.

Хорошо, грамотно, «культурно» составленный конспект лекции - одно из основных условий успешной работы студента в вузе.

Практические занятия – особая, специфичная для вуза форма учебной работы. Целью практические занятия является углублением и конкретизацией знаний и развитие навыков самостоятельного анализа вопросов по наиболее важным и сложным темам учебных курсов. На занятии преподаватель осуществляет контроль за самостоятельной работой студента в течение семестра. Его результаты фиксируются в учебных журналах, а затем в конце семестра являются основанием для получения зачета.

В процессе самостоятельной работы по дисциплине студент должен активно воспринимать, осмысливать и углублять полученную информацию, овладевать профессионально необходимыми умениями. Самым основным методом самостоятельной работы студента, на котором следует остановиться - это метод самостоятельного изучения литературы. Место, занимаемое им в процессе обучения, определяется теми особенностями, которые имеет чтение печатного текста по сравнению со слушанием устного изложения. При чтении нет принудительного темпа. Студент сам устанавливает его в зависимости от целей, характера литературного источника и своей подготовленности. Таким образом, при чтении создаются благоприятные условия для всестороннего осмысления и закрепления учебного материала.

Зачет является завершающим звеном в учебном процессе. Его результат в огромной степени зависит от того, насколько правильно студент организовал свою самостоятельную работу в течение семестра, насколько серьезно он занимался на практических занятиях. Начиная подготовку к зачету надо распределить время так, чтобы отработать все ответы, на контрольные вопросы, выносимые на зачёт и оставить день - два на окончательное повторение материала.

При подготовке контрольных вопросов целесообразно определить план изучения материала и строго ему следовать. Крайне нежелательно заниматься в ночное время накануне зачета так как это только внесет сумбур в уже полученные знания.

Ответ на зачете должен показать глубину понимания проблемы, знание фактического материала, первоисточников, умение логично, точно излагать свои мысли, оперировать научными понятиями и технологией.

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Лекции проводятся в лекционной аудитории, оборудованной проектором, экраном, учебной доской, ноутбуком. Техническое обеспечение: аудитория с мультимедийным оборудованием, которое используется в учебном процессе.

Лабораторные занятия проводятся в компьютерном классе, с выходом в Интернет и доступом в электронную информационно-образовательную среду университета.

Самостоятельная работа обучающихся осуществляется в помещениях, оснащенных компьютерной техникой с выходом в Интернет и доступом в электронную информационно-образовательную среду университета.