МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению самостоятельных работ по дисциплине

ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Направление подготовки	**10.03.01 Информационная безопасность**
Профиль	Комплексная защита объектов информатизации
Квалификация выпускника	бакалавр
Форма обучения	очная
Учебный план	2020 г.

Пятигорск, 2020 г.

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ 3
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ 3
3. СВЯЗЬ С ПРЕДШЕСТВУЮЩИМИ ДИСЦИПЛИНАМИ 3
4. СВЯЗЬ С ПОСЛЕДУЮЩИМИ ДИСЦИПЛИНАМИ 3
5. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ.....3
6. ТЕХНОЛОГИЧЕСКАЯ КАРТА САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТА.....4
7. СОДЕРЖАНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ.....5
8. КРИТЕРИИ ОЦЕНИВАНИЯ Компетенций.....6
9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ.....7

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью изучения дисциплины «Защита информационных процессов в компьютерных системах» является:

- изучение правовых основ защиты информации в компьютерных системах;
- изучение методов и средств защиты информации в компьютерных системах;
- ознакомления с методами противодействия утечке информации.

В курс включены основные методы защиты информации в компьютерных системах и стандарты оценки защищенности таких систем. В результате изучения курса студенты должны ознакомиться с основными стандартами, необходимыми для построения защищенных информационных систем.

В соответствии с указанной целью при изучении дисциплины «Защита информационных процессов в компьютерных системах» ставятся следующие задачи:

- ознакомление с основными понятиями и проблемами защиты информации в компьютерных системах;
- обучение методам защиты информации в компьютерных системах для построения защищенных информационных технологий.
- изучение правовых основ защиты информации в компьютерных системах;
- изучение методов и средств защиты информации в компьютерных системах;
- ознакомление с методами противодействия утечки информации;
- ознакомление с основными угрозами информации в компьютерных системах;
- изучение специфики возникновения угроз в открытых сетях;
- освоение особенностей защиты информации на узлах компьютерной сети;
- освоение системных вопросов защиты программ и данных;
- изучение основных категорий требований к программной и программно-аппаратной реализации средств защиты информации;
- изучение требований к защите автоматизированных систем от НСД.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Защита информационных процессов в компьютерных системах» входит в вариативную часть профессионального цикла ООП ВО подготовки бакалавра направления информационная безопасность, профиль подготовки – комплексная защита объектов информатизации. Ее освоение происходит в 7,8 семестрах.

3. СВЯЗЬ С ПРЕДШЕСТВУЮЩИМИ ДИСЦИПЛИНАМИ

Дисциплина базируется на ранее приобретенных студентами знаниями, полученными при изучении дисциплин естественнонаучного и профессионального цикла: теория информации, дискретная математика, информатика, математические основы криптологии.

4. СВЯЗЬ С ПОСЛЕДУЮЩИМИ ДИСЦИПЛИНАМИ

Освоение данной дисциплины происходит на завершающей стадии обучения. Связи с последующими дисциплинами нет.

5. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Индекс	Формулировка:
ПК-3	способность использовать нормативные правовые документы в своей профессиональной деятельности
ПК-4	способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности
ПК-5	способность организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты

	информации
ПК-6	способность организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов
ПК-8	способность определять виды и формы информации, подверженной угрозам, виды возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия
ПК-12	проектно-технологическая деятельность: способность участвовать в разработке подсистемы управления информационной безопасностью
ПК-13	способность к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности
ПК-21	способность проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов
ПК-25	организационно-управленческая деятельность: способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью
ПК-26	способность формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью
ПК-28	способность изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации
ПК-29	способность участвовать в работах по реализации политики информационной безопасности
ПК-30	способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности
ПК-33	способность организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю

6. ТЕХНОЛОГИЧЕСКАЯ КАРТА САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТА

Код реализуемой компетенции	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Обьем часов
7 семестр				
ПК-3, ПК-4, ПК-5, ПК-6, ПК-8, ПК-12, ПК-13, ПК-21, ПК-25, ПК-26, ПК-28, ПК-29, ПК-30, ПК-33	Самостоятельное изучение литературы по темам 2,3,9,11,12.	Конспект	Собеседование	8
ПК-3, ПК-4, ПК-5, ПК-6, ПК-8, ПК-12, ПК-13, ПК-21, ПК-25, ПК-26, ПК-28, ПК-29, ПК-30, ПК-33	Подготовка к лабораторным работам 1-8	Индивидуальное задание	Отчет письменный	8
ПК-3, ПК-4, ПК-5, ПК-6, ПК-8, ПК-12, ПК-13, ПК-21, ПК-25, ПК-26, ПК-28, ПК-29, ПК-30, ПК-33	Подготовка к практическим занятиям 1-8	Индивидуальное задание	Отчет письменный	8
ПК-3, ПК-4, ПК-5, ПК-6, ПК-8, ПК-12, ПК-13, ПК-21, ПК-25, ПК-26, ПК-28, ПК-29, ПК-30, ПК-33	Подготовка и выполнение курсового проекта	Курсовой проект	Защита курсового проекта	10

			Итого за 7 семестр:	34
8 семестр				
ПК-3, ПК-4, ПК-5, ПК-6, ПК-8, ПК-12, ПК-13, ПК-21, ПК-25, ПК-26, ПК-28, ПК-29, ПК-30, ПК-33	Самостоятельное изучение литературы по темам 18,22.	Конспект	Собеседование	4
ПК-3, ПК-4, ПК-5, ПК-6, ПК-8, ПК-12, ПК-13, ПК-21, ПК-25, ПК-26, ПК-28, ПК-29, ПК-30, ПК-33	Подготовка к лабораторным работам 9-15	Индивидуальное задание	Отчет письменный	4
			Итого за 8 семестр:	8
			Итого:	42

7. СОДЕРЖАНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Тема 2. Основные понятия и положения защиты информации в КС.

Содержание:

Понятие информационной безопасности. Субъект и объект информационной системы. Классификация информационных ресурсов. Понятие доступа к информации.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-4	1-4

Оценочные средства: собеседование

Тема 3. Правовые основы защиты информации информационных процессов в компьютерных системах.

Содержание:

Стандарты и рекомендации, образующие базис понятий, на котором строятся работы по обеспечению информационной безопасности. Стратегия и доктрина национальной безопасности РФ в информационной сфере.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-4	1-4

Оценочные средства: собеседование

Тема 9. Защита информации в АС обработки данных.

Содержание:

Анализ электромагнитных излучений и наводок в компьютерных системах. Характеристики излучения протоколов обмена. Анализ спектра протоколов обмена.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-4	1-4

Оценочные средства: собеседование

Тема 11. Обзор методов защиты информационных процессов в компьютерных системах.

Содержание:

Причины, влияющие на развитие в области защиты информации. Методы защиты информации.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-4	1-4

Оценочные средства: собеседование

Тема 12. Организационные методы защиты информационных процессов в компьютерных системах.

Содержание:

Организационно-административные методы защиты информации. Организационно-технические методы защиты информации. Физические средства защиты информации. Страхование как метод защиты информации.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-4	1-4

Оценочные средства: собеседование

Тема 18. Канальный, сетевой, транспортный уровни модели взаимодействия открытых систем.

Содержание:

Рекомендации, позволяющие дополнительно защитить компьютерную сеть предприятия средствами канального уровня. Протоколы сетевого уровня. Межсетевой экран.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-4	1-4

Оценочные средства: собеседование

Тема 22. Основные виды работ администрирования серверных систем и приложений.

Содержание:

Настройка и администрирование сервера. Настройка системы безопасности, контроль и отчеты по трафику. Классическое администрирование. Адаптация инфраструктуры к нуждам приложений. Автоматизация управления ПО. Обеспечение информационной безопасности СУБД. Уровень полномочий субъекта. Дискреционная защита.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-4	1-4

Оценочные средства: собеседование

8. КРИТЕРИИ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Оценка «отлично» выставляется студенту, если глубокие, исчерпывающие знания и творческие способности в понимании, изложении и использовании учебно-программного материала; логически последовательные, содержательные, полные, правильные и конкретные ответы на все поставленные вопросы и дополнительные вопросы преподавателя; свободное владение основной и дополнительной литературой, рекомендованной учебной программой.

Оценка «хорошо» выставляется студенту, если твердые и достаточно полные знания всего программного материала, правильное понимание сущности и взаимосвязи рассматриваемых процессов и явлений; последовательные, правильные, конкретные ответы на поставленные вопросы при свободном устранении замечаний по отдельным вопросам; достаточное владение литературой, рекомендованной учебной программой.

Оценка «удовлетворительно» выставляется студенту, если твердые знания и понимание основного программного материала; правильные, без грубых ошибок ответы на поставленные вопросы при устранении неточностей и несущественных ошибок в освещении отдельных положений при наводящих вопросах преподавателя; недостаточное владение литературой, рекомендованной учебной программой.

Оценка «неудовлетворительно» выставляется студенту, если неправильные ответы на основные вопросы, допущены грубые ошибки в ответах, непонимание сущности излагаемых вопросов; неуверенные и неточные ответы на дополнительные вопросы.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1. Рекомендуемая литература

9.1.1. Основная литература:

1. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях: учебное пособие – М.: ДМК Пресс, 2014. – 592 с.
2. Бабаш А.В. Информационная безопасность. Лабораторный практикум: учебное пособие. – М.: КноРус, 2012.

9.1.2. Дополнительная литература:

1. Чипига А.Ф. Информационная безопасность автоматизированных систем: учебное пособие. – М.: Гелиос АРВ, 2010.
2. Громов Ю.Ю. Информационная безопасность и защита информации: учебное пособие. – Старый Оскол: ТНТ, 2010.

9.1.3. Методическая литература:

1. Методические указания по выполнению лабораторных работ по дисциплине «Защита информационных процессов в компьютерных системах».
2. Методические указания по выполнению практических работ по дисциплине «Защита информационных процессов в компьютерных системах».
3. Методические указания по выполнению курсового проекта по дисциплине «Защита информационных процессов в компьютерных системах».
4. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «Защита информационных процессов в компьютерных системах».

9.1.4. Интернет-ресурсы:

1. http://www.intuit.ru – сайт дистанционного образования в области информационных технологий.
2. http://window.edu.ru – образовательные ресурсы ведущих вузов.
3. http://ncfu.ru – сайт СКФУ.
4. http://www.consultant.ru/ – нормативно-правовая документация.

9.1.5. Программное обеспечение

Операционная система Windows версия XP и выше, браузер Internet Explorer или любой другой, интегрированный пакет Microsoft.

9.2. Материально-техническое обеспечение дисциплины

Лабораторные занятия проводятся в компьютерных классах, в которых установлена программа Microsoft Visual Studio 2010, 2012, а также другие системы для разработки программных приложений.