Аннотация к рабочей программе дисциплины «Основы информационной безопасности»

Цель преподавания дисциплины

Целью преподавания дисциплины «Основы информационной безопасности» получение студентами знаний о принципах построения, идеологии и архитектуре механизмов обеспечения информационной безопасности, а также создание предпосылок для использования полученных знаний в профессиональной деятельности.

Задачи изучения дисциплины

Основными обобщенными задачами дисциплины являются:

- ознакомление с основными понятиями информационной безопасности;
- приобретение знаний об основных направлениях защиты информации;
- изучение законодательной базы Российской Федерации в области защиты информации;
- приобретение знаний о современных методах и средствах защиты информации в информационно-телекоммуникационных и автоматизированных системах;
- получить знания об архитектуре защищённых автоматизированных систем.

Компетенции, формируемые в результате освоения дисциплины

- способность к работе в коллективе и кооперации с коллегами;
-способностями к освоению новых образцов программных, технических средств и информационных технологий;
-защиты и восстановления работоспособности, подсистем информационной безопасности автоматизированной системы;
-формирования позиции в сфере профессиональной деятельности;
-способность организовать работу по поиску необходимого материала;
-четко формулировать свои мысли при формировании позиции;
-защиты и восстановления работоспособности, подсистем информационной безопасности автоматизированной системы.

У обучающихся формируются следующие компетенции:

- способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);

- способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем (ПК-1).

Разделы дисциплины

Введение в информационную безопасность. Понятие защищенности в автоматизированных системах. Основы законодательства РФ в области информационной безопасности и защиты информации. Конфиденциальная информация и ее защита. Лицензирование и сертификация в области обеспечения безопасности информации. Технические средства обеспечения информационной безопасности. Электромагнитные каналы утечки информации. Электромагнитные каналы утечки информации. Угроза безопасности информации АСОД и субъектов информационных отношений

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Декан факультета
фундаментальной и прикладной
(наименование ф-та полностью)
информатики

Т.А. Ширабакина
(подпись, инициалы, фамилия)
«____» _____ 20___ г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности

направление подготовки (специальность) *10.05.02*
(шифр согласно ФГОС
Информационная безопасность телекоммуникационных систем
и наименование направление подготовки (специальности)

Защита информации в системах связи и управления
наименование профиля, специализации или магистерской программы

форма обучения *очная*
очная, очно-заочная, заочная

Курск – 20*17*

2

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего профессионального образования направления подготовки *10.05.02 – « Информационная безопасность телекоммуникационных систем»* и на основании учебного плана направления подготовки *10.05.02 – « Информационная безопасность телекоммуникационных систем»*, одобренного Учёным советом университета, протокол № 5 «30» 01 2017 г.

Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по направлению подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»* на заседании кафедры информационной безопасности.
«28» августа 2017 г. Протокол № 1

И.о. зав. кафедрой ИБ Таныгин М.О.

Разработчик программы
доцент кафедры ИБ Марухленко А.Л.

Согласовано:
Директор научной библиотеки Макаровская В.Г.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол № 5 «30» 01 2017 г. на заседании кафедры информационной безопасности. Протокол № 12 «29» 06 2018 г.
Зав. кафедрой Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол № 5 «30» 01 2017 г. на заседании кафедры информационной безопасности. Протокол № 12 «29» 06 2018 г.
Зав. Кафедрой к.т.н., доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана по специальности *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол № 5 «30» 01 2019 г. на заседании кафедры информационной безопасности. Протокол № 11 «27» 06 2019 г.
Зав. кафедрой к.т.н., доцент Таныгин М.О.

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_7_ «_25_» _02_ 20_20_ г. на заседании кафедры информационной безопасности. Протокол №_1_ от «_31_» _08_ 20_20_г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_7_ «_25_» _02_ 20_20_ г. на заседании кафедры информационной безопасности. Протокол №_11_ от «_28_» _06_ 20_21_г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №_7_ «_25_» _02_ 20_20_ г. на заседании кафедры информационной безопасности. Протокол №_11_ от «_30_» _06_ 20_22_г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.05.02 – «Информационная безопасность телекоммуникационных систем»*, одобренного Ученым советом университета протокол №__ «___» _____ 20__ г. на заседании кафедры информационной безопасности. Протокол №__ от «__»_____20__г.

Зав. кафедрой _____

1. Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

1.1. Цель дисциплины

Целью преподавания дисциплины «Основы информационной безопасности» получение студентами знаний о принципах построения, идеологии и архитектуре механизмов обеспечения информационной безопасности, а также создание предпосылок для использования полученных знаний в профессиональной деятельности.

1.2. Задачи дисциплины

Основными обобщенными задачами дисциплины являются:

- ознакомление с основными понятиями информационной безопасности;
- приобретение знаний об основных направлениях защиты информации;
- изучение законодательной базы Российской Федерации в области защиты информации;
- приобретение знаний о современных методах и средствах защиты информации в информационно-телекоммуникационных и автоматизированных системах;
- получить знания об архитектуре защищённых автоматизированных систем.

1.3 Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Обучающиеся должны **знать:**

– основные необходимые компоненты для организации коммуникативной функции в устной и письменной формах на русском;

– как восстановить работоспособность системы защиты информации при возникновении нештатных ситуаций;

– основы устной и письменной речи;

– основные принципы системы информационной безопасности, основные направления деятельности;

– основные необходимые компоненты для организации коммуникативной функции в устной и письменной формах на русском и иностранном языках.

уметь:

– вырабатывать управленческие решения в сфере профессиональной деятельности;

– в качестве руководителя подразделения, формировать цели команды, принимать организационно-управленческие решения в ситуациях риска и нести за них ответственность;

– организовывать работу для решения задач межличностного и межкультурного взаимодействия;

– осуществлять подбор, изучение и обобщение научно-технической литературы; находить необходимую информацию из различных источников;

– Четко и ясно излагать свои мысли;

– работу по обобщению научно-технической литературы, нормативных и методических материалов.

владеть :

– способность к работе в коллективе и кооперации с коллегами;

– способностями к освоению новых образцов программных, технических средств и информационных технологий;

– защиты и восстановления работоспособности, подсистем информационной безопасности автоматизированной системы;

– формирования позиции в сфере профессиональной деятельности ;

– способность организовать работу по поиску необходимого материала;

– четко формулировать свои мысли при формировании позиции;

– защиты и восстановления работоспособности, подсистем информационной безопасности автоматизированной системы.

У обучающихся формируются следующие компетенции:

- способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);

- способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем (ПК-1).

2. Указание места дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам вариативной части профессионального цикла (Б1.Б.32). Изучается на 2 курсе в 4 семестре.

3. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоёмкость (объём) дисциплины составляет 3 зачётные единицы, 108 часов

Таблица 3 – Объём дисциплины

Виды учебной работы	Всего, часов
Общая трудоемкость дисциплины	108
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	37,15
Лекции	18
лабораторные занятия	18
практические занятия	не предусмотрено
экзамен	1,15
зачет	не предусмотрено
курсовая работа (проект)	не предусмотрено
расчетно-графическая (контрольная) работа	не предусмотрено
Аудиторная работа (всего):	36
в том числе:	
лекции	18
лабораторные занятия	18
практические занятия	0
Самостоятельная работа обучающихся (всего)	34,85
Контроль/экз (подготовка к экзамену)	36

4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1	2	3
1.	Введение в информационную безопасность	Цели и задачи информационной безопасности. Ввод в профессию. Понятия информация, информатизация, информационная система, информационная безопасность. Принципы обеспечения информационной безопасности
2.	Понятие защищенности в автоматизированных системах	Понятие защищенность АСОД. Факторы защищенности АСОД. Меры защиты информации. Правовое обеспечение информационной безопасности.
3.	Основы законодательства РФ в	Основы законодательства РФ в области информационной безопасности и защиты информации. Государственная

	области информационной безопасности и защиты информации	тайна, коммерческая тайна, служебная тайна, профессиональная тайна, персональные данные. Режимы секретности.
4.	Конфиденциальная информация и ее защита	Конфиденциальная информация и ее защита. Коммерческая тайна. Служебная тайна. Профессиональная тайна. Персональные данные. Подразделение данных.
5.	Лицензирование и сертификация в области обеспечения безопасности информации	Лицензирование. Сертификация. Подтверждение соответствия. Организационное обеспечение информационной безопасности.
6.	Технические средства обеспечения информационной безопасности	Средства вычислительной техники. Технические средства разведки. Технические средства и системы.
7.	Электромагнитные каналы утечки информации	Побочные электромагнитные излучения ТСПИ. Побочные электромагнитные излучения на частотах работы высокочастотных генераторов ТСПИ. Паразитная генерация .
8.	Электрические каналы утечки информации	Причины возникновения электрических каналов утечки информации. Способы и средства подавления электронных устройств перехвата речевой информации.
9.	Угроза безопасности информации АСОД и субъектов информационных отношений	Угроза. Нарушитель. Нарушение. Классификация угроз безопасности. Классификация каналов проникновения в систему и утечки информации. Неформальная модель нарушителя в АСОД.

Таблица 4.1.2– Содержание дисциплины и ее методическое обеспечение

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек., час	№ пр.	№ лб.			
1	2	3	4	5	6	7	8
1.	Введение в информационную безопасность	2	-	1	У-2,3, М-1	С	ОК-5, ПК-1
2.	Понятие защищенности в автоматизированных системах	2	-	2	У-1,4, М-2	КО, С	ОК-5, ПК-1
3.	Основы законодательства РФ в области информационной безопасности и защиты информации	2	-	3	О-1,3 Д-7-12, М-3	КО	ОК-5, ПК-1
4.	Конфиденциальная информация и ее защита	2	-	4	У-5,6,7, М-4	13 КО	ОК-5, ПК-1

1	2	3	4	5	6	7	8
5.	Лицензирование и сертификация в области обеспечения безопасности информации	2	-	5	У-2,3,9, М-5	18 КО, С	ОК-5, ПК-1
6.	Технические средства обеспечения информационной безопасности	2	-	6	У-1,2,3,8, М-6	КО	ОК-5, ПК-1
7.	Электромагнитные каналы утечки информации	2	-	7	О-1,3, Д-2-7, , М-7	С	ОК-5, ПК-1
8.	Электрические каналы утечки информации	2	-	8	О-1,2, Д-1-4, , М-8	КО	ОК-5, ПК-1
9.	Угроза безопасности информации АСОД и субъектов информационных отношений	2	-	9	У-1,3,4, М-9	КО	ОК-5, ПК-1
	Итого	18		9			

Э – экзамен, КР – курсовая работа; КП – курсовой проект, К – контрольная работа, З – зачет, С – собеседование, СР – семестровая работа, Кл – коллоквиум, КО – контрольный опрос, МК – автоматизированный программированный контроль (машинный контроль).

4.2Лабораторные работы и (или) практические занятия

4.2.1.Лабораторные работы

Таблица 4.2.1 – Лабораторные работы

	Наименование лабораторной работы	Объем, час.
1.	Лабораторная работа №1 – Виды информации и основные методы ее защиты	2
2.	Лабораторная работа №2 – Виды угроз информационной безопасности Российской Федерации	2
3.	Лабораторная работа №3 – Источники угроз информационной безопасности Российской Федерации.	2
4.	Лабораторная работа №4 – Исследование атаки переполнения буфера как примера нарушения конфиденциальности, целостности и доступности информации	2
5.	Лабораторная работа №5 – Причины, виды, каналы утечки и искажения информации	2
6.	Лабораторная работа №6 – Защита от утечек по каналу ПЭМИН, по акустическому и виброакустическому каналам	2
7.	Лабораторная работа №7 - Сетевое сканирование	2
8.	Лабораторная работа №8 - Анализ трафика и сбор критичной информации программами пассивного анализа	2
9.	Лабораторная работа №9 - Аудит комплексной защиты информации предприятия	2

Итого	18

4.1.2. Практические занятия

не предусмотрены

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.3 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1.	Введение.	4	4
2.	Цели и задачи информационной безопасности. Ввод в профессию. Понятия информация, информатизация, информационная система, информационная безопасность. Принципы обеспечения информационной безопасности	4	4
3.	Понятие защищенность АСОД. Факторы защищенности АСОД. Меры защиты информации. Правовое обеспечение информационной безопасности.	3,85	3,85
4.	Основы законодательства РФ в области информационной безопасности и защиты информации.	3,5	3,5
5.	Государственная тайна, коммерческая тайна, служебная тайна, профессиональная тайна, персональные данные. Режимы секретности	3,5	3,5
6.	Конфиденциальная информация и ее защита. Коммерческая тайна. Служебная тайна. Профессиональная тайна. Персональные данные. Подразделение данных.	2	2
7.	Лицензирование. Сертификация. Подтверждение соответствия. Организационное обеспечение информационной безопасности.	2	2
8.	Средства вычислительной техники. Технические средства разведки. Технические средства и системы.	2	2
9.	Побочные электромагнитные излучения ТСПИ. Побочные электромагнитные излучения на частотах работы высокочастотных генераторов ТСПИ. Паразитная генерация .	2	2
10.	Причины возникновения электрических каналов утечки информации. Способы и средства подавления электронных устройств перехвата речевой информации.	2	2
11.	Угроза. Нарушитель. Нарушение. Классификация угроз безопасности. Классификация каналов проникновения в систему и утечки информации. Неформальная модель нарушителя в АСОД.	2	2

12.	Подготовка реферата по предлагаемым темам (по выбору студента).	4	4
Итого			34,85

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплин пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

– библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с данной РПД;

– имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

– путем обеспечения доступности всего необходимого учебно-методического и справочного материала за счёт выкладывания на сайт кафедры ИБ в интернете (адрес http://www.swsu.ru/structura/up/fivt/k_ib/index.php);

– путем предоставления сведений о наличии учебно-методической литературы, современных программных средств;

– путем разработки вопросов к экзамену

– методических указаний к выполнению лабораторных работ.

типографией университета

– путем помощи авторам в подготовке и издании научной, учебной, учебно-методической литературы.

6. Образовательные технологии

В соответствии с требованиями ФГОС и Приказа Министерства образования и науки РФ от 05 апреля 2017 г. №301 по направлению подготовки 10.03.01 «Информационная безопасность» реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. Удельный вес занятий, проводимых в интерактивных формах, составляет 22,2 процента от аудиторных занятий согласно УП.

Таблица 6.1 – Интерактивные образовательные технологии, используемые при проведении аудиторных занятий

№	Наименование раздела (темы лекции, практического или лабораторного занятия)	Используемые интерактивные образовательные технологии	Объём, час.
1.	Выполнение лабораторной работы – Источники угроз информационной безопасности Российской Федерации.	Разбор конкретных ситуаций	2
2.	Выполнение лабораторной работы - Исследование атаки переполнения буфера как примера нарушения конфиденциальности, целостности и доступности информации	Разбор конкретных ситуаций	2
3.	Выполнение лабораторной работы – Причины, виды, каналы утечки и искажения информации	Разбор конкретных ситуаций	2
4.	Выполнение лабораторной работы – Защита от утечек по каналу ПЭМИН, по акустическому и виброакустическому каналам	Разбор конкретных ситуаций	1
5.	Выполнение лабораторной работы - Сетевое сканирование	Разбор конкретных ситуаций	1
	Итого		8

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код и содержание компетенции	Этапы* формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать	Планирование профессиональной карьеры Практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности	Основы информационной безопасности Введение в специальность	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

нормы профессиональной этики (ОК-5).			
способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем (ПК-1)	Русский язык и культура речи Практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности Учебно-лабораторный практикум	Информационная безопасность телекоммуникационных систем Основы информационной безопасности Основы криптографии Основы теории чисел Научно-исследовательская работа	Планирование и управление информационной безопасностью Основы многоканальных систем передачи Системы и сети радиосвязи Системы и сети мобильной связи Ознакомительная практика Практика по получению профессиональных умений и опыта профессиональной деятельности Преддипломная практика Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описания шкал оценивания

Наименование компетенции	Критерии освоения		
	Пороговый уровень («удовлетвори-тельно)	Продвинутый уровень (хорошо»)	Высокий уровень («отлично»)
ОК-5 способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения	**Знать**: основные принципы системы информационной безопасности, основные направления деятельности. **Уметь**: вырабатывать управленческие решения в сфере профессиональной деятельности **Владеть навыками**: способность к работе в	**Знать**: основные принципы системы информационной безопасности, основные направления деятельности. **Уметь**: в качестве руководителя подразделения, формировать цели команды, принимать организационно-	**Знать**: основные принципы системы информационной безопасности; как восстановить работоспособность системы защиты информации при возникновении нештатных ситуаций **Уметь**: организовывать работу малых

информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	коллективе и кооперации с коллегами	управленческие решения в ситуациях риска и нести за них ответственность **Владеть навыками**: к освоению новых образцов программных, технических средств и информационных технологий	коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности **Владеть навыками**: защиты и восстановления работоспособности, подсистем информационной безопасности автоматизированной системы
ПК-1 способностью осуществлять анализ научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем	**Знать**: основы устной и письменной речи; основные принципы системы информационной безопасности, основные направления деятельности. **Уметь:** четко, ясно излагать свои мысли **Владеть навыками**: формирования позиции в сфере профессиональной деятельности ; способность организовать работу по поиску необходимого материала	**Знать**: основные необходимые компоненты для организации коммуникативной функции в устной и письменной формах на русском **Уметь**: осуществлять подбор, изучение и обобщение научно-технической литературы; находить необходимую информацию из различных источников **Владеть навыками**: четкого, лаконичного изложения мыслей	**Знать:** основные необходимые компоненты для организации коммуникативной функции в устной и письменной формах на русском и иностранном языках **Уметь:** работу по обобщению научно-технической литературы, нормативных и методических материалов **Владеть навыками:** четко формулировать свои мысли при формировании позиции; защиты и восстановления работоспособности, подсистем информационной безопасности автоматизированной системы.

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля

№ п/п	Раздел (тема) дисциплины	Код контролируемой компетенции (или её части)	Технология форматирования	Оценочные средства		Описание шкал оценивания
				наименование	№ заданий	
1	2	3	4	5	6	7
1	Введение в информационную безопасность	ОК-5, ПК-1	Лекция, СРС, Лабораторная работа	Собеседование		Согласно табл. 7.2
2	Понятие защищенности в автоматизированных системах	ОК-5, ПК-1	Лекция, СРС, Лабораторная работа	Рефераты		Согласно табл. 7.2
				Контрольные вопросы к лаб №1		
3	Основы законодательства РФ в области информационной безопасности и защиты информации	ОК-5, ПК-1	Лекция, СРС, Лабораторная работа	Тест		Согласно табл. 7.2
4	Конфиденциальная информация и ее защита	ОК-5, ПК-1	Лекция, СРС, Лабораторная работа	Собеседование		Согласно табл. 7.2
5	Лицензирование и сертификация в области обеспечения безопасности информации	ОК-5, ПК-1	Лекция, СРС, Лабораторная работа	Собеседование		Согласно табл. 7.2
				Тест		
				Контрольные вопросы к лаб №2,3		
6	Технические средства обеспечения информационной безопасности	ОК-5, ПК-1	Лекция, СРС, Лабораторная работа	Собеседование		Согласно табл. 7.2
7	Электромагнитные каналы утечки информации	ОК-5, ПК-1	Лекция, СРС, Лабораторная работа	Тест		Согласно табл. 7.2
8	Электрические каналы утечки информации	ОК-5, ПК-1	Лекция, СРС, Лабораторная работа	Рефераты		Согласно табл. 7.2
9	Угроза безопасности информации АСОД и субъектов информационных отношений	ОК-5, ПК-1	Лекция, СРС, Лабораторная работа	Собеседование		Согласно табл. 7.2

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулирующих следующими нормативными актами университета:

- Положение П 02.016 – 2015 «О балльно-рейтинговой системе оценки качества освоений образовательных программ»;
- методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля* по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

Форма контроля	Минимальный балл		Максимальный балл	
	балл	примечание	балл	примечание
Лабораторная работа №1 – Виды информации и основные методы ее защиты	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Лабораторная работа №2 – Виды угроз информационной безопасности Российской Федерации	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Лабораторная работа №3 – Источники угроз информационной безопасности Российской Федерации.	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Лабораторная работа №4 – Исследование атаки переполнения буфера как примера нарушения конфиденциальности, целостности и доступности информации	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Лабораторная работа №5 – Причины, виды, каналы утечки и искажения информации	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Лабораторная работа №6 – Защита от утечек по каналу ПЭМИН, по акустическому и виброакустическому каналам	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»

Лабораторная работа №7 - Сетевое сканирование	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Лабораторная работа №8 - Анализ трафика и сбор критичной информации программами пассивного анализа	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
Лабораторная работа №9 - Аудит комплексной защиты информации предприятия	1	Выполнил, но «не защитил»	2	Выполнил и «защитил»
СРС	10		20	
Итого	24		48	
Посещаемость	0		16	
Экзамен	0		36	
Итого	24		100	

При итоговом контроле в форме бланкового теста студенту предлагается 15 вопросов по различным темам курса. Полученную итоговую сумму условных баллов (максимум 15) переводят в баллы на экзамене (максимум 36) путём умножения на 2.4 и округления до целого значения.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1) Синицын, Сергей Владимирович . Операционные системы [Текст] : учебник / С. В. Синицын, А. В. Батаев, Н. Ю. Налютин. - 2-е изд., испр. - М. : Академия, 2012. - 304 с.

2) Фороузан Б. А. Математика криптографии и теория шифрования [Электронный ресурс] : учебник / Б. А. Фороузан. - М. : НОУ «Интуит», 2016. - 511 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=428998

3) Лапонина, О. Р. Криптографические основы безопасности [Электронный ресурс] : учебная литература / О.Р. Лапонина. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 244 с. - Режим доступа : http://biblioclub.ru/index.php?page=book&id=429092

4) Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник / О. В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. - Режим доступа : http://biblioclub.ru/index.php?page=book&id=438331

8.2. Дополнительная учебная литература

1) Котова Л. В. Сборник задач по дисциплине «Методы и средства защиты информации»[Текст] : учебное пособие / Л.В. Котова. - М. : МПГУ, 2015. - 44 с. - (Основы информационной безопасности). - ISBN 978-5-4263-0221-1

2) Технические средства и методы защиты информации [Текст] : учебное пособие / под ред. А. П. Зайцева и А. А. Шелупанова. - Москва : Горячая линия - Телеком, 2012. - 616 с. : ил. - ISBN 978-5-9912-00 84-4

3) Информационная безопасность в государственных и негосударственных структурах "Информтех-2012" [Текст] : сборник материалов II Всероссийской научно-практической конференции с международным участием, 28-30 мая 2012 г. / Юго-Западный гос. ун-т ; ред. кол.: В. П. Добрица (отв. ред.) [и др.]. - Курск : ЮЗГУ, 2012. - 192 с. - ISBN 978-5-7681-07 47-5

4) Информатика. Базовый курс [Текст] : учебное пособие / под ред. С. В. Симоновича. - 3-е изд. - СПб. : Питер, 2012. - 640 с. : ил. - (Учебник для вузов). - ISBN 978-5-459-004 39-7

5) Мельников, В. П. Информационная безопасность и защита информации [Текст] : учебное пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков. - М. : Академия, 2006. - 336 с.

6) Гаврилов, М. В. Осмотр при расследовании преступлений в сфере компьютерной информации [Текст] : монография / М. В. Гаврилов, А. Н. Иванов. - М. : Юрлитинформ, 2008. - 168 с.

7) Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С. А. Нестеров ; Министерство образования и науки Российской Федерации, Санкт-Петербургский государственный политехнический университет. - СПб. : Издательство Политехнического университета, 2014. - 322 с. - Режим доступа : http://biblioclub.ru/index.php?page=book&id=363040

8.3. Перечень методических указаний

1. Виды информации и основные методы ее защиты: методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун-т; сост.: А.Л. Марухленко. Курск, 2017. 8с.

2. Виды угроз информационной безопасности Российской Федерации: методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун-т; сост.: А.Л. Марухленко. Курск, 2017. 7с.

3. Источники угроз информационной безопасности Российской Федерации.: методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун-т; сост.: А.Л. Марухленко. Курск, 2017. 8с.

4. Исследование атаки переполнения буфера как примера нарушения конфиденциальности, целостности и доступности информации: методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун-т; сост.: А.Л. Марухленко. Курск, 2017. 10с.

5. Причины, виды, каналы утечки и искажения информации: методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун-т; сост.: А.Л. Марухленко. Курск, 2017. 11с.

6. Защита от утечек по каналу ПЭМИН, по акустическому и виброакустическому каналам: методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун-т; сост.: А.Л. Марухленко. Курск, 2017. 7с.

7. Сетевое сканирование: методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун-т; сост.: А.Л. Марухленко. Курск, 2017. 6с.

8. Анализ трафика и сбор критичной информации программами пассивного анализа: методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун-т; сост.: А.Л. Марухленко. Курск, 2017. 6с.

9. Аудит комплексной защиты информации предприятия: методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун-т; сост.: А.Л. Марухленко. Курск, 2017. 8с.

9. Перечень ресурсов информационно-телекоммуникационной сети Интернет

1. Корпорация Microsoft [официальный сайт]. Режим доступа: http://www.microsoft.com/
2. Перечень ресурсов информационно-телекаммуникационной сети «Интернет», необходимых для освоения дисциплины

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины «Основы информационной безопасности» являются лекции и практические работы. Студент не имеет права пропускать занятия без уважительных причин.

На лекциях излагаются и разъясняются основные понятия темы, связанные с ней теоретические и практические проблемы, даются рекомендации для самостоятельной работы. В ходе лекции студент должен внимательно слушать и конспектировать материал.

Изучение наиболее важных тем или разделов дисциплины завершают практические работы, которые обеспечивают: контроль подготовленности студента; закрепление учебного материала; приобретение опыта устных

публичных выступлений, ведения дискуссии, в том числе аргументации и защиты выдвигаемых положений и тезисов.

Практической работе предшествует самостоятельная работа студента, связанная с освоением материала, полученного на лекциях, и материалов, изложенных в учебниках и учебных пособиях, а также литературе, рекомендованной преподавателем.

По согласованию с преподавателем или по его заданию студенты готовят рефераты по отдельным темам дисциплины, выступают на занятиях с докладами. Основу докладов составляет, как правило, содержание подготовленных студентами рефератов.

Качество учебной работы студентов преподаватель оценивает по результатам тестирования, собеседования, защиты отчетов по практическим работам, а также по результатам докладов.

Преподаватель уже на первых занятиях объясняет студентам, какие формы обучения следует использовать при самостоятельном изучении дисциплины «Основы информационной безопасности»: конспектирование учебной литературы и лекции, составление словарей понятий и терминов и т. п.

В процессе обучения преподаватели используют активные формы работы со студентами: чтение лекций, привлечение студентов к творческому процессу на лекциях, промежуточный контроль путем отработки студентами пропущенных лекции, участие в групповых и индивидуальных консультациях (собеседовании). Эти формы способствуют выработке у студентов умения работать с учебником и литературой. Изучение литературы составляет значительную часть самостоятельной работы студента. Это большой труд, требующий усилий и желания студента. В самом начале работы над книгой важно определить цель и направление этой работы. Прочитанное следует закрепить в памяти. Одним из приемов закрепление освоенного материала является конспектирование, без которого немыслима серьезная работа над литературой. Систематическое конспектирование

помогает научиться правильно, кратко и четко излагать своими словами прочитанный материал.

Самостоятельную работу следует начинать с первых занятий. От занятия к занятию нужно регулярно прочитывать конспект лекций, знакомиться с соответствующими разделами учебника, читать и конспектировать литературу по каждой теме дисциплины. Самостоятельная работа дает студентам возможность равномерно распределить нагрузку, способствует более глубокому и качественному усвоению учебного материала. В случае необходимости студенты обращаются за консультацией к преподавателю по вопросам дисциплины «Основы информационной безопасности» с целью усвоения и закрепления компетенций.

Основная цель самостоятельной работы студента при изучении дисциплины «Основы информационной безопасности» - закрепить теоретические знания, полученные в процессе лекционных занятий, а также сформировать практические навыки самостоятельного анализа особенностей дисциплины.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

- Microsoft Office 2016.Лицензионный договор №S0000000722 от 21.12.2015 г. с ООО «АйТи46», лицензионный договор №K0000000117 от 21.12.2015 г. с ООО «СМСКанал»;
- Kaspersky Endpoint Security Russian Edition, лицензия 156A-140624-192234;
- Windows 7, договор IT000012385.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Учебная аудитория для проведения занятий лекционного и практического типа или лаборатории кафедры информационная безопасность, оснащенные мебелью: столы, стулья для обучающихся; стол,

стул для преподавателя; доска, проектор для демонстрации презентаций. Помещение для самостоятельной работы Компьютер PDC2160/iC33/2*512Mb/HDD 160Gb/DVD-ROM/FDD/ATX350W/ K/m/OFF/l 7 TFT E700 (6 шт).

13 Лист дополнений и изменений, внесенных в рабочую программу дисциплины

Номер изменения	Номера страниц				Всего страниц	дата	Основание для изменения и подпись лица, проводившего изменения
	измененных	заменённых	аннулированных	новых			

ПРИЛОЖЕНИЕ А Образец билета в тестовой форме

ЮГО-ЗАПАДНЫЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет ФиПИ Утверждено на заседании
Направление подготовки кафедры ИБ,
10.05.02 Протокол № __ от ____ 201__ г.
курс 2, семестр 4 Зав. кафедрой _____М.О. Таныгин
Дисциплина «Основы информационной безопасности»

1. Из перечисленного базовыми услугами для обеспечения безопасности компьютерных систем и сетей являются
1) аутентификация;
2) идентификация;
3) целостность;
4) контроль доступа;
5) контроль трафика;
6) причастность.

2. Готовность устройства к использованию всякий раз, когда в этом возникает необходимость, характеризует свойство:
1) Целостность;
2) Доступность;
3) Детерминированность;
4) Восстанавливаемость.

3. Защита информации от утечки это деятельность по предотвращению:
1) Несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации;
2) Воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;
3) Неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;
4) Воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации
5) Получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации

4. *Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:*
1) Подстановки;
2) Аналитических преобразований;
3) Кодирования;
4) Гаммирования

5) Перестановки

5. *Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:*
1) Доктор;
2) Ревизор;
3) Сторож;
4) Детектор
5) Сканер.

6. Гарантия сохранности данными правильных значений, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом модифицировать, разрушать или создавать данные -- это
1) Доступность;
2) Детерминированность;
3) Целостность.
4) Восстанавливаемость

7. Информация - это
1) Только сведения, содержащиеся в электронных базах данных;
2) Только документированные сведения о лицах, предметах, фактах, событиях;
3) Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.
4) Сведения, поступающие от СМИ

8. Защита информации это:
1) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
2) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
3) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.
4) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям
5) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа

9. Что такое политика безопасности?
1) Пошаговые инструкции по выполнению задач безопасности;
2) Детализированные документы по обработке инцидентов безопасности;
3) Общие руководящие требования по достижению определенного уровня безопасности.
4) Широкие, высокоуровневые заявления руководства

10. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?
1) AS/NZS;
2) Анализ связующего дерева;
3) NIST.
4) Анализ сбоев и дефектов

11. Информация
1) Становится доступной, если она содержится на материальном носителей;
2) Характеризуется всеми перечисленными свойствами;
3) Не исчезает при потреблении.
4) Подвергается только "моральному износу"

12. Перехват данных является угрозой
1) Целостности;
2) Доступности;

3) Конфеденциальности.
13. *Естественные угрозы безопасности информации вызваны* 1) Воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека; 2) Ошибками при проектировании АСОИ, её элементов или разработке программного обеспечения; 3) Корыстными устремлениями злоумышленников. 4) Деятельностью человека 5) Ошибками при действиях персонала
14. Что такое процедура? 1) Пошаговая инструкция по выполнению задачи; 2) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах; 3) Обязательные действия. 4) Правила использования программного и аппаратного обеспечения в компании.
15. Искусственные угрозы безопасности информации вызваны: 1) Ошибками при действиях персонала; 2) Корыстными устремлениями злоумышленников; 3) Ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения. 4) Деятельностью человека 5) Воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека
Экзаменатор _____Марухленко А.Л.