Аннотация к рабочей программе дисциплины «Основы информационной безопасности»

Цель преподавания дисциплины

Целью преподавания дисциплины «Основы информационной безопасности» изучается с целью ознакомления студентов с современным состоянием теории безопасности информационных систем, правовым регулированием в области защиты информации, принципами, алгоритмами и методами организации защиты информации в организациях и предприятиях различных направлений деятельности и различных форм собственности.

Задачи изучения дисциплины

– ознакомление с принципами, базовыми определениями и вариантами организации защиты информации;

– ознакомление с актуальной нормативно-правовой базой РФ по части информационной безопасности;

– изучение угроз информационной безопасности, моделей поведения злоумышленника, основ работы с конфиденциальными данными;

– ознакомление с основами защиты авторских прав, работы с персональными данными;

– изучения способов выявления контрафактной продукции;

– изучение, в том числе на практическом уровне, основ криптографических преобразований в части потоковых шифров, ассиметричных систем и перспективных методов защиты;

– ознакомление с технологиями защиты программного обеспечения.

Компетенции, формируемые в результате освоения дисциплины

Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства (ОПК-

1);

Разделы дисциплины

Базовые понятия. Конфиденциальность. Классификация угроз. Угрозы ИБ. Классы нарушителей. Оценка риска. Персональные данные. Защита авторских прав. Выявление контрафактной продукции. Криптографические методы защиты.

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

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

Т.А. Ширабакина
(подпись, инициалы, фамилия)
«01» 02 2017 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы информационной безопасности

направление подготовки (специальность) *10.03.01*
(шифр согласно ФГОС
Информационная безопасность
и наименование направление подготовки (специальности)

Безопасность автоматизированных систем
наименование профиля, специализации или магистерской программы

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

Курск – 2017

Рабочая программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность и на основании учебного плана направления подготовки 10.03.01 Информационная безопасность , одобренного Учёным советом университета, протокол №5 «30» января 2017 г.

Рабочая программа обсуждена и рекомендована к применению в учебном процессе для обучения студентов по направлению подготовки 10.03.01 Информационная безопасность на заседании кафедры информационной безопасности № 9 «1» февраля 2017г.

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 направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол №5 «30» января 2017г. на заседании кафедры информационной безопасности 28.08.2017, №1
(наименование кафедры, дата, номер протокола)

Зав. кафедрой к.т.н., доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол №9 «26» марта 2018г. на заседании кафедры информационной безопасности 29.06.2018, №12
(наименование кафедры, дата, номер протокола)

Зав. кафедрой к.т.н., доцент Таныгин М.О.

Рабочая программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки 10.03.01 Информационная безопасность, одобренного Ученым советом университета протокол №5 «26» 03 2019г. на заседании кафедры информационной безопасности 27.06.2019, №11
(наименование кафедры, дата, номер протокола)

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 *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №1 от «31» 08 2020г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «28» 06 2021 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, одобренного Ученым советом университета протокол №7 «25» 02 2020 г. на заседании кафедры информационной безопасности. Протокол №11 от «30» 06 2022 г.

Зав. кафедрой _____

Программа пересмотрена, обсуждена и рекомендована к применению в образовательном процессе на основании учебного плана направления подготовки *10.03.01 – «Информационная безопасность»*, 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 *10.03.01 – «Информационная безопасность»*, 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, соотнесённых с планируемыми результатами освоения образовательной программы

1.1. Цель дисциплины

Дисциплина «Основы информационной безопасности» изучается с целью ознакомления студентов с современным состоянием теории безопасности информационных систем, правовым регулированием в области защиты информации, принципами организации аппаратно-программных способов защиты информации в организациях и предприятиях различных направлений деятельности и различных форм собственности.

1.2. Задачи дисциплины

Основными задачами изучения учебной дисциплины являются приобретение студентами познаний в области:

– защиты безопасности;

– информационной безопасности – сравнительно молодой, быстро развивающейся области информационных технологий (словосочетание «информационная безопасность» в разных контекстах может иметь различный смысл);

– защищенности национальных интересов в информационной сфере;

– правильного подхода к проблемам информационной безопасности, который начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС).

1.3. Перечень планируемых результатов обучения, соотнесённых с планируемыми результатами освоения образовательной программы

В процессе изучения дисциплины «Основы информационной безопасности» происходит формирование следующих общекультурных и профессиональных компетенций:

- 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 к самоорганизации и самообразованию (ОК-8).

2. Указание места дисциплины в структуре образовательной программы

«Основы информационной безопасности» (Б1.Б.Б13) является частью учебного плана направления подготовки 10.03.01 «Информационная безопасность». Изучается на 1 курсе в 1 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 2 зачётных единицы, 72 академических часов.

Таблица 3.1 – Объём дисциплины по видам учебных занятий

Общая трудоемкость дисциплины	72
Контактная работа обучающихся с преподавателем (по видам учебных занятий) (всего)	36,1
Лекции	18
лабораторные занятия	0
практические занятия	18
Экзамен	не предусм.
зачет	0,1
курсовая работа (проект)	не предусм.
расчетно-графическая (контрольная) работа	не предусм.
Аудиторная работа (всего):	36
в том числе:	
Лекции	18
лабораторные занятия	0
практические занятия	18
Самостоятельная работа обучающихся (всего)	35,9
Контроль/экз (подготовка к экзамену)	

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 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Введение в информационную безопасность	Информационная сфера (среда). Целостность Доступность. Конфиденциальность. Основные принципы обеспечения информационной безопасности. Системность подхода. Комплексность подхода. Принцип разумной достаточности.
2.	Понятие защищенности в автоматизированных системах	Понятие защищенности. Меры и средства защиты информации

3.	Основы законодательства РФ в области информационной безопасности и защиты информации	Федеральный закон «Об информации, информационных технологиях и о защите информации». государственная тайна. следующая система обозначения сведений: «Особой важности», «Совершенно секретно», «Секретно».
4.	Конфиденциальная информация и ее защита	Коммерческая тайна. Служебная тайна. Профессиональная тайна. Персональные данные
5.	Лицензирование и сертификация в области обеспечения безопасности информации	Лицензирование. Организационное обеспечение информационной безопасности. Организационные (административные) средства защиты.
6.	Технические средства обеспечения информационной безопасности	Основные технические средства. Вспомогательные технические средства и системы
7.	Электромагнитные каналы утечки информации	Побочные электромагнитные излучения ТСПИ. Побочные электромагнитные излучения на частотах работы высокочастотных генераторов ТСПИ. Паразитная генерация (побочные электромагнитные излучения, возникающие вследствие паразитной генерации в элементах ТСПИ)
8.	Электрические каналы утечки информации	Причинами возникновения электрических каналов утечки информации. Способы и средства подавления электронных устройств перехвата речевой информации
9.	Угроза безопасности информации АСОД и субъектов информационных отношений	Угроза интересов субъекта информационных отношений. Классификация угроз безопасности. Классификация каналов проникновения в систему и утечки информации. При контактном НСД. При бесконтактном НСД. Неформальная модель нарушителя в АСОД

Таблица 4.2 – 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	№ лб	№ пр.			
1	2	3	4	5	6	7	8
1	Введение в информационную безопасность	2		1	О-1,2 Д-1,2 М-1	С(1-2)	ОК-5
2	Понятие защищенности в автоматизированных системах	2		2	О-1,3 Д-3-4 М-2	КО(3-4)	ОК-5
3	Основы законодательства РФ в области информационной безопасности и защиты информации	2		3	О-1,2 Д-1,3 М-3	КО(5-6)	ОК-5 ОК-8

№ п/п	Раздел (тема) дисциплины	Виды деятельности			Учебно-методические материалы	Формы текущего контроля успеваемости *(по неделям семестра)*	Компетенции
		лек. час	№ лб	№ пр.			
1	2	3	4	5	6	7	8
4	Конфиденциальная информация и ее защита	2		4	О-1,2 Д-1,3 М-4	С(7-8)	ОК-8
5	Лицензирование и сертификация в области обеспечения безопасности информации	2		5	О-2 Д-4 М-5	С(9-10)	ОК-8
6	Технические средства обеспечения информационной безопасности	2		6	О-2 Д-3 М-6	С(11-12)	ОК-5
7	Электромагнитные каналы утечки информации	2		7	О-3, Д-4 М-7	С(13-14)	ОК-5 ОК-8
8	Электрические каналы утечки информации	2		8	О-1 Д-2 М-8	КО(15-16)	ОК-8
9	Угроза безопасности информации АСОД и субъектов информационных отношений	2		9	О-1,3, Д-2-4 М-9	К(17-18)	ОК-5 ОК-8
	Итого	18		18			

К – контрольная работа, С – собеседование, КО – контрольный опрос

4.2. Лабораторные работы и (или) практические занятия

4.2.1. Практические занятия

Таблица 4.3. – Практические занятия

	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

4.3. Самостоятельная работа студентов (СРС)

Таблица 4.4 – Самостоятельная работа студентов

№	Наименование раздела учебной дисциплины	Срок выполнения	Время, затрачиваемое на выполнение СРС, час.
1	2	3	4
1.	Введение в информационную безопасность	1-2 недели	4
2.	Понятие защищенности в автоматизированных системах	3-4 недели	4
3.	Основы законодательства РФ в области информационной безопасности и защиты информации	5-6 недели	4
4.	Конфиденциальная информация и ее защита	7-8 недели	4
5.	Лицензирование и сертификация в области обеспечения безопасности информации	9-10 недели	4
6.	Технические средства обеспечения информационной безопасности	11-12 недели	4
7.	Электромагнитные каналы утечки информации	13-14 недели	4
8.	Электрические каналы утечки информации	15-16 недели	2
9.	Угроза безопасности информации АСОД и субъектов информационных отношений	17-18 недели	2
10.	Подготовка к зачету	1-18 недели	3,9
Итого			35,9

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;

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

– путем разработки вопросов к зачету, методических указаний к выполнению практических работ.

типографией университета:

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

– путем удовлетворения потребностей в тиражировании 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 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 24.9% от аудиторных занятий согласно УП. Средствами промежуточного контроля успеваемости студентов являются защита работ, опросы на практических занятиях по темам лекций.

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,	Разбор конкретных ситуаций	2

	целостности и доступности информации		
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	2
5.	Выполнение лабораторной работы - Сетевое сканирование	Разбор конкретных ситуаций	2
	Итого		10

7. Фонд оценочных средств для проведения промежуточной аттестации

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

Таблица 7.1 – Этапы формирования компетенций

Код и содержание компетенции	Этапы формирования компетенций и дисциплины (модули), при изучении которых формируется данная компетенция		
	начальный	основной	завершающий
1	2	3	4
ОК-5 способность 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	**Знать**: основные принципы системы информационной безопасности, основные направления деятельности. **Уметь**: вырабатывать управленческие решения в сфере профессиональной деятельности **Владеть навыками**: способность к работе в коллективе и кооперации с коллегами	**Знать**: основные принципы системы информационной безопасности, основные направления деятельности. **Уметь**: в качестве руководителя подразделения, формировать цели команды, принимать организационно-управленческие решения в ситуациях риска и нести за них ответственность **Владеть навыками**: к освоению новых образцов программных,	**Знать**: основные принципы системы информационной безопасности; как восстановить работоспособность системы защиты информации при возникновении нештатных ситуаций **Уметь**: организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности **Владеть навыками**: защиты и восстановления работоспособности,

		технических средств и информационных технологий	подсистем информационной безопасности автоматизированной системы
ОК-8 способностью к самоорганизации и самообразованию	**Знать**: основы устной и письменной речи **Уметь:** четко, ясно излагать свои мысли **Владеть навыками**: формирования позиции в сфере профессиональной деятельности	**Знать**: основные необходимые компоненты для организации коммуникативной функции в устной и письменной формах на русском **Уметь**: 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:** организовывать работу для решения задач межличностного и межкультурного взаимодействия **Владеть навыками:** четко формулировать свои мысли при формировании позиции

7.2. 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 компетенции (или её части)	Технология формирования	Оценочные средства	Описание шкал оценивания
				наименование	
1	2	3	4	5	6
1	Введение в информационную безопасность	ОК-5 ОК-8	Лекция, практические занятия, СРС	Собеседование	В соответствии с таблицей 7.2

2	Понятие защищенности в автоматизированных системах	ОК-5 ОК-8	Лекция, практические занятия, СРС	Контрольный опрос	В соответствии с таблицей 7.2
3	Основы законодательства РФ в области информационной безопасности и защиты информации	ОК-5 ОК-8	Лекция, практические занятия, СРС	Контрольный опрос	В соответствии с таблицей 7.2
4	Конфиденциальная информация и ее защита	ОК-5 ОК-8	Лекция, практические занятия, СРС	Собеседование	В соответствии с таблицей 7.2
5	Лицензирование и сертификация в области обеспечения безопасности информации	ОК-5 ОК-8	Лекция, практические занятия, СРС	Собеседование	В соответствии с таблицей 7.2
6	Технические средства обеспечения информационной безопасности	ОК-5	Лекция, практические занятия, СРС	Собеседование	В соответствии с таблицей 7.2
7	Электромагнитные каналы утечки информации	ОК-5	Лекция, практические занятия, СРС	Собеседование	В соответствии с таблицей 7.2
8	Электрические каналы утечки информации	ОК-5	Лекция, практические занятия, СРС	Контрольный опрос	В соответствии с таблицей 7.2
9	Угроза безопасности информации АСОД и субъектов информационных отношений	ОК-5	Лекция, практические занятия, СРС	Контрольная работа	В соответствии с таблицей 7.2

7.3. Рейтинговый контроль изучения учебной дисциплины

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

– Положение П 02.016–2015 «О балльно-рейтинговой системе оценки качества освоения 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) Технологии защиты информации в компьютерных сетях. Межсетевые экраны и интернет-маршрутизаторы [Текст] : учебное пособие / Е. А. Богданова [и др.]. - Москва : Национальный Открытый Университет "ИНТУИТ", 2013. - 743 с. - (Основы информационных технологий). - ISBN 978-5-9556-01 42-7

2) Ищейнов, Вячеслав Яковлевич. Защита конфиденциальной информации [Текст] : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. - Москва : Форум, 2013. - 256 с. : ил. - (Высшее образование). - ISBN 978-5-91134-3 36-1.

3) Спеваков, А. Г. Основы правового обеспечения информационной безопасности [Текст] : учебное пособие / А. Г. Спеваков, А. П. Фисун ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2013 - .Ч. 1. - 150 с. : ил., табл. - Имеется электрон. аналог. - Библиогр.: с. 137-149. - ISBN 978-5-7681-08 57-1.

4) Загинайлов Ю. Н. Теория информационной безопасности и методов за-щиты информации [Электронный ресурс] : учеб. пособие / Ю. Н. Загинайлов. – М .: Директ-Медиа, 2015. – 253с. Режим доступа : http://biblioclub.ru/index.php?page=book_red&id=276557

8.2. Дополнительная литература

1) Организационно-правовое обеспечение информационной безопасности [Текст] : учебное пособие / под ред. А. А. Стрельцова. - М. : Академия, 2008. - 256 с. - (Высшее профессиональное образование). - ISBN 978-5-7695-42 40-4.

2) Романов, О. А. Организационное обеспечение информационной безопасности [Текст] : учебник / О. А. Романов, С. А. Бабин, С. Г. Жданов. - М. : Академия, 2008. - 192 с. - (Высшее профессиональное образование). - ISBN 978-5-7695-42 72-5

3) Рябко, Борис Яковлевич. Основы современной криптографии и стенографии [Текст] : монография / Б. Я. Рябко, А. Н. Фионов. - М. : Горячая линия-Телеком, 2010. - 232 с. : ил. - ISBN 978-5-9912-01 50-6

4) Спицин В. Г. Информационная безопасность вычислительной техники [Электронный ресурс] : учебное пособие / Спицин В. Г. - Томск : Эль-Контент, 2011. - 148 с. - Режим доступа : http://biblioclub.ru/index.php?page=book_red&id=208694

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, необходимых для освоения дисциплины

1) Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/.

2) Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/

3) Электронная библиотека ЮЗГУ (http:// http://lib.swsu.ru)

4) Электронно-библиотечная система Университетская библиотека онлайн (https://biblioclub.ru)

10. Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы студента при изучении дисциплины являются лекции и практические занятия. 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 занятия, 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.

Практическому занятию 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 готовить рефераты по отдельным темам дисциплины, выступать 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: 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.

Самостоятельная работа студентов включает в себя изучение материалов дисциплины по записям лекций и учебникам, выполнение домашних заданий, оформление отчетов по практическим работам и практическим занятиям, подготовку рефератов по заданным темам, а также подготовку к зачету. Вся эта работа планируется самим студентом по рекомендациям преподавателя.

Студенты, не имеющие опыта и считающие, что можно работать без плана, запускают занятия и, будучи не в состоянии нагнать пропущенное, перестают понимать лекции, не справляются с решением задач на практических занятиях.

Оценка результативности самостоятельной работы студентов обеспечивается контрольными опросами и собеседованиями со студентами и проверкой выполнения заданий по преподавателя.

Рекомендуется следующий порядок работы студента. Сначала выполняется наиболее трудная ее часть: изучение учебного материала по записям лекций, прослушанных в этот же день. Прочтя свою запись и дополнив ее тем, что еще свежо в памяти, студент обращается к учебнику по дисциплине или к электронному ресурсу. Рекомендуется делать выписки из источников информации на свободных страницах конспекта. В процессе проработки материала отмечаются неясные стороны изучаемой темы и формулируются вопросы, которые следует задать преподавателю.

Наилучшего результата достигают те студенты, которые предварительно знакомятся с материалом по теме предстоящих занятий.

Благодаря этому студенты будут осознанно и критически относиться к изложению лекции и воспримут ее с большим “коэффициентом полезного действия”.

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
	Изменённых	заменённых	аннулированных	новых			

ПРИЛОЖЕНИЕ А Образец билета в тестовой форме

ЮГО-ЗАПАДНЫЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет ФиПИ
Направление подготовки 10.03.01
курс 1, семестр 1
Дисциплина «Основы информационной безопасности»

Утверждено на заседании кафедры ИБ,
Протокол № __ от ____ 201__ г.
Зав. кафедрой _____М.О. Таныгин

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.