Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Дагестанский государственный технический университет»

РЕКОМЕНДОВАНО
К УТВЕРЖДЕНИЮ
Декан, председатель совета
факультета КТВТиЭ
_____ Ш. А. Юсуфов
«18» 10 2018 г.

УТВЕРЖДАЮ
Проректор по учебной работе,
председатель методического совета
ДГТУ
_____ Н. С. Суракатов
«19» 10 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина Б1.В.ДВ.6 Защита электронного документооборота
(наименование дисциплины по учебному плану)

Специальность 10.05.03 «Информационная безопасность автоматизированных систем»

Специализация «Безопасность открытых информационных систем»

Факультет Компьютерных технологий, вычислительной техники и энергетики
(наименование факультета, где ведется дисциплина)

Кафедра Информационная безопасность
(наименование кафедры, за которой закреплена дисциплина)

Квалификация выпускника бакалавр

Форма обучения очная, курс 4 семестр(ы) 7

Всего трудоемкость в зачетных единицах (часах) 2 ЗЕ (72 часов)

лекции 17 (час); экзамен - (семестр)

практические (семинарские) занятия 17 (час); зачет 7 (семестр)

лабораторные занятия - (час); самостоятельная работа 38 (час);

курсовой проект (работа), РГР - (семестр).

Зав. кафедрой ИБ _____ Г.Н. Качаева
(подпись)

Начальник УО _____ Э.В. Магомаева
(подпись)

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.03- «Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем».

Программа одобрена на заседании выпускающей кафедры от «15» октября 2018года, протокол № 2.

Зав. выпускающей кафедрой по данной специальности _____ **Г.И.Качаева**

ОДОБРЕНО:

Методической комиссией по укрупненным группам специальностей и направлению подготовки

10.00.00- «Информационная безопасность»

Председатель МК

_____ Мелехин В.Ф.

«15» 10 2018г.

АВТОР (Ы) ПРОГРАММЫ:

_____ Качаева Г.И., к.э.н., ст. преп. каф. ИБ

1. Цели и задачи освоения дисциплины «Защита электронного документооборота»

Дисциплина "Защита электронного документооборота" реализует требования федерального государственного образовательного стандарта высшего образования по специальности 10.05.03- «Информационная безопасность автоматизированных систем. специализация «Безопасность открытых информационных систем».

Целью дисциплины является формирование у обучающихся по специальности 10.05.03- «Информационная безопасность автоматизированных систем» знаний. умений. навыков и опыта деятельности. характеризующих этапы формирования компетенций и обеспечивающих достижение планируемых результатов освоения образовательной программы.

Приобретенные знания позволят студентам основывать свою профессиональную деятельность на процессном подходе. формировать требования к системе управления ИБ конкретного объекта. принимать участие в проектировании системы управления ИБ. принимать участие в эксплуатации системы управления ИБ.

Задачами дисциплины являются:

- Формирование требований к системе управления ИБ конкретного объекта.
- Проектирование системы управления ИБ конкретного объекта.
- Эффективное управление ИБ конкретного объекта.

Таким образом. дисциплина "Защита электронного документооборота" является неотъемлемой составной частью профессиональной подготовки по направлению подготовки 10.03.01 «Информационная безопасность автоматизированных систем». Вместе с другими дисциплинами цикла профессиональных дисциплин изучение данной дисциплины призвано формировать специалиста. и в частности. вырабатывать у него такие качества. как:

- строгость в суждениях.
- творческое мышление.
- организованность и работоспособность.
- дисциплинированность.
- самостоятельность и ответственность

2. Место дисциплины «Защита электронного документооборота» в структуре ООП специалитета

Дисциплина «Защита электронного документооборота» относится к обязательным дисциплинам вариативной части.

Дисциплина "Защита электронного документооборота" основывается на знаниях. полученных при изучении дисциплин: «Основы информационной безопасности».
Дисциплина «Защита электронного документооборота» обеспечивает изучение дисциплин: «Организационное и правовое обеспечение информационной безопасности». Знания и практические навыки. полученные из дисциплины «Защита электронного документооборота». используются обучаемыми при разработке выпускных квалификационных работ.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины «Защита электронного документооборота»

Изучение дисциплины «Гуманитарные аспекты информационной безопасности» обеспечивает овладение следующими компетенциями:

Общекультурные компетенции (ОК):

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);

результате изучения дисциплины студент должен:

знать:

- *основные понятия информатики;*
- *место и роль информационной безопасности в системе национальной безопасности Российской Федерации;*

уметь:

- *анализировать мировоззренческие, социально и личностно значимые философские проблемы;*
- *проводить исторический анализ событий, анализировать и оценивать социальную информацию; планировать и осуществлять свою деятельность с*
- *учетом результатов этого анализа;*

владеть:

- *навыками письменного аргументированного изложения собственной точки зрения;*
- *навыками публичной речи, аргументации, ведения дискуссии и полемики, практического анализа логики различного рода рассуждений;*
- *навыками критического восприятия информации;*

4.Структура и содержание дисциплины(модуля) «Защита электронного документооборота»

Общая трудоемкость дисциплины составляет 2 зачетные единицы – 72 часа, в том числе: лекционных -17 часов, практических - 17 часов, СРС – 38 часов, форма отчетности зачет в 7 семестре.

4.1. Содержание дисциплины

№ п/п	Раздел дисциплины Тема лекции и вопросы	Семестр	Недели семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля (по срокам текущей аттестации)
				ЛК	ПЗ	ЛР	СРС	
1	2	3	4	5	6	7	8	9
1.	**Лекция 1. Тема Введение в дисциплину. Гуманитарные проблемы информационной безопасности** Информационное общество: общественный прогресс и новые реальности. Содержание и взаимосвязи понятий «информационная безопасность» и «национальная безопасность». Национальная безопасность России в условиях информационного общества. Понятие международной информационной безопасности. Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации	7	1,2	2	2		4	Вх. контр.
2.	**Лекция 2. Тема: Гуманитарные проблемы информационной безопасности** Информационно-психологическая безопасность как составляющая информационной безопасности. Информационная сфера как системообразующий фактор жизни общества. Доктрина информационной безопасности Российской Федерации.	7	3,4	2	2		4	

	Информационное обеспечение государственной политики. Сохранение культурно-нравственных ценностей российского народа. Подходы к оцениванию информационной безопасности России.							
3.	**Лекция 3. Тема: Общие сведения об информационно- психологической безопасности.** Информационные взаимосвязи личности, общества и государства. Информационные воздействия на личность, общество и государство. Возможности применения информационных воздействий деструктивного характера для нанесения ущерба личности, обществу и государству. Понятие и структура информационно-психологической безопасности. Субъекты, объекты и источники угроз информационно-психологической безопасности.	7	5,6	2	2		4	АКР№1
4.	**Лекция 4. Тема: Информационно-психологическая безопасность.** Информационное противоборство и информационная война. Понятия информационного и рефлексивного управления, их роль в информационном обществе. Модели информационного и рефлексивного управления. Понятия информационного и информационно-психологического противоборства. Теоретические основы информационного противоборства. Информационная война как средство достижения политических целей. Информационное оружие. Взгляды иностранных государств на информационную войну. Информационные войны в новейшей истории. Основы государственной информационной политики в условиях информационно-психологической войны.	7	7,8	2	2		6	
5.	**Лекция 5. Тема: Информационное противоборство и информационная война.** Информационные воздействия как инструмент скрытого управления личностью и обществом. Информационные воздействия различных	7	9,10	2	2		4	АКР№2

	коммуникативных ситуациях. Модели, ресурсы, технологии и мишени информационных воздействий. Основные типы и содержание технологий информационного воздействия. Понятие и примеры манипулирования в различных областях социального взаимодействия.							
6.	**Лекция 6. Тема: Информационное противоборство и информационная война.** Способы манипулирования в массовых информационных процессах. в ходе обсуждений и дискуссий.в межличностном общении. Ложь какередство манипулирования. Слухи и провокации как способы информационно-психологического воздействия. Глобальная сеть Интернет как среда реализации информационных воздействий деструктивного характера.	7	11.12	2	2		4	
7.	**Лекция 7. Тема: Информационные воздействия как инструмент скрытого управления личностью и обществом.** Технологии скрытого управления личностью и обществом с помощью информационных воздействий. Информационно-психологические операции как комплексные организационные технологии скрытого управления. Информационно-психологические операции в современных вооружённых конфликтах. Информационно-психологические операции в избирательных кампаниях. «Кризисные» технологии как вид информационно-психологических операций. Технология постепенного изменения общественного сознания (модель «окна Овертона»). Политика ненасильственных действий как метод влияния на внутриполитические отношения. Технологии управления личностью, применяемые в тоталитарных сектах и деструктивных культах. Информационные операции в сети Интернет.	7	13.14	2	2		4	
8.	**Лекция 8. Тема: Основы обеспечения информационно-психологической безопасности личности.**	7	15.16	2	2		4	АКР№3

	Общие сведения об информационно-психологической защите личности. Основные направления обеспечения информационно-психологической безопасности личности. Понятие и виды психологической защиты личности. Понятие и структура системы психологической защиты личности. Инструментарий оценки информационно-психологической защищенности личности. Алгоритмические основы психологической самозащиты личности.							
9.	**Лекция 9. Тема: Основы обеспечения информационно-психологической безопасности личности.** Основные формы психологической самозащиты. Основы психологической самозащиты в межличностных, контакт-коммуникативных, масс-коммуникативных ситуациях и при работе в глобальной сети Интернет. Способы повышения стрессоустойчивости личности. Алгоритмический подход к организации психологической самозащиты.	7	17	1	1		4	
	Итого			**17**	**17**		**38**	**Зачет**

4.2.Содержание практических занятий

№	№ лекции из рабочей программы	Наименование и содержание практического занятия	Литература (№ источника из табл. прил. 12)	Кол-во часов
1	№1	***Введение. Понятие информационной безопасности.*** Существующие стандарты и методологии по управлению ИБ: их отличия, сильные и слабые стороны (на примере семейства стандартов ISO IEC 2700x, СТО БР ИББС - 1.0, ГОСТ Р ИСО МЭК 17799, ГОСТ Р ИСО МЭК 27001, ISO IEC 18044, ISO IEC 25999 и др.).	1-5	2
2	№2	***Составляющие ИБ*** - Разработка и управление политикой Иь информационной системы	1-5	4
3	№ 3	***Нормативные документы в области ИБ*** - Анализ модели угроз Иь и уязвимостей - Анализ модели информационных потоков	1-5	2
4	№ 4	***Структура и задачи органов обеспечивающих ИБ*** -Процессы улучшения СУИь («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия») - Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса». -Процесс «Анализ со стороны высшего руководства». -Процесс «Обучение и обеспечение осведомленности».	5-8	2
5	№ 5	***Эксплуатация и независимый аудит СУИь*** Сертификация по ISO IEC 27001 или ГОСТ Р ИСО МЭК 27001. Период эксплуатации СУИь перед сертификацией. Органы по сертификации, работающие в РФ их различия и требования). Этапы сертификационного аудита. Решение о сертификации	5-8	2
6	№ 6	***ИБ: конфиденциальность, целостность, доступность.*** Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости».	7,8	2

		Цель документа. Структура и содержание документа. Процесс разработки документа, решение спорных ситуаций при разработке документа.		
7	№ 7	***Организационно-технические и режимные меры и методы»*** Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.	2.3.5	2
8	№ 8	***Обеспечение соответствия требованиям законодательства РФ*** Разработка процессов или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены)	7.8	2
9	№ 9	***Основы обеспечения информационно-психологической безопасности личности.*** Основные формы психологической самозащиты. Основы психологической самозащиты в межличностных, контакт-коммуникативных, масс-коммуникативных ситуациях и при работе в глобальной сети Интернет. Способы повышения стрессоустойчивости личности. Алгоритмический подход к организации психологической самозащиты.		1
Итого				17

4.3.Тематика для самостоятельной работы студентов

№	Содержание дисциплины, самостоятельно изучаемое студентами	Кол-во Часов из содержания дисциплины	Рекомендуемая литература и источники информации	Формы контроля (контр. работа, практич. и лаб. занятия и т.д..)
1.	Введение в дисциплину. Гуманитарные проблемы информационной безопасности	4	№1.2	Опрос, реферат, статья
2.	Гуманитарные проблемы информационной безопасности	4	№1-8	Опрос, реферат, статья
3.	Общие сведения об информационно-психологической безопасности.	4	№1-8	Опрос, реферат, статья

4.	Информационно-психологическая безопасность.	6	№1-8	Опрос, реферат, статья
5.	Информационное противоборство и информационная война.	4	№1-8	Опрос, реферат, статья
6.	Информационное противоборство и информационная война.	4	№1-8	Опрос, реферат, статья
7.	Информационные воздействия как инструмент скрытого управления личностью и обществом.	4	№1-8	Опрос, реферат, статья
8.	Основы обеспечения информационно-психологической безопасности личности.	4		Опрос, реферат, статья
9.	Основы обеспечения информационно-психологической безопасности личности.	4		Опрос, реферат, статья
Итого		**38**		

5.Образовательные технологии

В соответствии с требованиями ФГОС РД по направлению подготовки реализация компетентностного подхода должна предусматривать широкое использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При проведении занятий по учебной дисциплине рекомендуется следовать и традиционным технологиям, в частности, в каждом разделе курса выделять наиболее важные моменты, акцентировать на них внимание обучаемых. При чтении лекций по всем разделам программы иллюстрировать теоретический материал большим количеством примеров, что позволит сделать изложение наглядным и продемонстрировать обучаемым приемы программирования.

Предусмотрено сочетание традиционных видов учебной активности, таких как конспектирование лекций и контроль усвоения теоретического материала в виде коллоквиумов, так и интерактивных технологий, таких как собеседования, ситуационные игры на выбор методов защиты информации на практических занятиях.

При изучении всех разделов программы добиться точного знания обучаемыми основных исходных понятий.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенностью контингента обучающихся и содержанием дисциплины, и целом в учебном процессе они должны составлять не менее 20 % аудиторных занятий (8ч).

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При изучении дисциплины «Защита электронного документооборота» информационные технологии применяются в следующих случаях:

- изучение информационных технологий сопровождения и выполнение практических работ (текстовые редакторы, электронные таблицы, базы данных, средства автоматизированного проектирования и др.);
- использование ресурсов Интернет для проведения поисково-аналитической работы;
- использование специализированного программного обеспечения, такого как: специальные редакторы и интегрированные среды (языки программирования, аудио, графические, видео и другие виды редакторов);
- программы компьютерного моделирования архитектурных проектов;
- программы для проведения численных расчетов и обработки результатов;
- оформление учебных и научных работ (рефератов, курсовых работ (проектов), мини-проектов, выступлений на семинаре, отчетов по лабораторному или практическому занятию и т.п.);
- демонстрация дидактических материалов с использованием мультимедийных технологий;
- использование информационно-справочного обеспечения, такого как правовые справочные системы (Гарант, Консультант + и др.), онлайн словари, справочники;
- использование специализированных справочных систем (электронных учебников, виртуальных экскурсий и справочников, коллекций иллюстраций и фотоизображений;
- использование на занятиях электронных изданий (графических объектов, видео-аудио- материалов (через Интернет), виртуальных лабораторий, практикумов);
- организация взаимодействия с обучающимися посредством электронной почты, форумов;
- использование видеоконференцсвязи.

Для данной дисциплины применяется следующее программное обеспечение и информационно-справочные системы:

1. Программное обеспечение:

Windows 8
Windows 10
MS Offise 2003
MS Offise 2010 Антивирус Касперского Антивирус.
Moodle – система управления ДО (GNU General Public License).
Adobe CLP CS6 Master Collection 6 Multiple Platforms Russian AOO License CLP Level

2. Информационные справочные системы и профессиональные базы данных:

ЭБС «Университетскаябиблиотекаонлайн».(URL:http://www.biblioclub.ru).
Базовая коллекция.
East View Information Services (ИстВью).ООО «ИВИС». (http://www.ebiblioteka.ru).
Доступ к базе данных «Издания по общественным и гуманитарным наукам».
Электронные образовательные ресурсы по дисциплине, размещенные в электронной образовательной среде университета dstu.ru.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно– методическое обеспечение самостоятельной работы студентов

6.1.Вопросы для входной контрольной работы

1. Что такое экономика?
2. Что представляет собой микроэкономика?
3. Роль экономики в жизни общества.
4. Какие проблемы должна решить экономика?
5. Кого мы называем субъектами рынка и что такой рынок?
6. Что такое потребность? Чем потребность отличается от нужды?

6.2.Контрольные работы по проверке текущих знаний студентов

Аттестационная контрольная работа №1

1. Цели и задачи управления ИБ.
2. Понятие системы управления. Понятие ИБ.
3. Место ИБ в рамках общей системы управления предприятием.
4. Типовые меры по защите информации от наблюдения.
5. Типовые меры по защите информации от подслушивания.
6. Типовые меры по защите информации от перехвата.
7. Понятие Политики СУИБ.
8. Цели Политики СУИБ.
9. Структура и содержание Политики СУИБ.
10. Источники информации для разработки Политики СУИБ.
11. Законодательные и нормативно-правовые акты Российской Федерации по защите информации.
12. Структура, задачи и основные функции Государственной системы защиты информации.

Аттестационная контрольная работа №2

1. Виды и способы конкуренции. Совершенная конкуренция.
2. Основные типы рыночных структур несовершенной конкуренции.
3. Чистая монополия. Естественная монополия. Ценовая дискриминация.
4. Монополия. Монопсония.
5. Олигополия. Олигопсония. Монополистическая конкуренция с дифференциацией продукта.
6. Антимонопольное законодательство и регулирование экономики: основные принципы.
7. Спрос на факторы производства и предложение в условиях совершенной конкуренции. Ценовая эластичность спроса на ресурсы.
8. Спрос и предложение на рынке труда.
9. Равновесие на рынке труда и равновесная ставка заработной платы.
10. Дифференциация ставок заработной платы.
11. Несовершенная конкуренция на рынке труда.
12. Понятие капитала. Спрос и предложение на рынке капитала.
13. Реальный и номинальный процент. Принцип дисконтирования. Ставки ссудного процента и инвестиционные решения.
14. Особенности предложения на рынке природных ресурсов. Земельная рента, цена земли.
15. Прибыль: нормальная и экономическая. Функции прибыли.
16. Макроэкономика как объект научного анализа. Макроэкономические агенты. Макроэкономические рынки.
17. Общественный продукт, сущность и структура. Валовый внутренний продукт (ВВП) и валовый национальный продукт (ВНП).
18. Методы расчета ВВП и ВНП. Дефлятор ВНП. Конечное и промежуточное потребление.

19. Чистый национальный продукт (ЧНП) и национальное богатство. Чисто экономическое благосостояние. Национальный доход (произведенный, использованный, личный, располагаемый).
20. Система национальных счетов. Соотношение показателей в системе национальных счетов.

Аттестационная контрольная работа №3

1. Документирование процесса внедрения разработанных процессов.
2. Типовой документ «Положение о применимости». Цель документа. Структура и содержание документа.
3. Процесс разработки документа, решение спорных ситуаций при разработке документа.
4. Участники процесса. Обязательные этапы процесса. Связи с другими процессами СУИБ.
5. Разработка процессов или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены).

Контрольные вопросы для проверки остаточных знаний.

1. Обеспечение информационной безопасности: содержание и структура понятия.
2. Информация, защищаемая информация, объект информатизации, информационные ресурсы, информационная технология.
3. Стандартизация в области построения СУИБ: сходства и различия стандартов.
4. Защита информации. Основные термины и определения.
5. Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему).
6. Модели угроз и нарушителей информационной безопасности.
7. Политика ИБ и политика СУИБ: сходства и различия.
8. Принципы защиты информации от НСД.
9. Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
10. Анализ рисков ИБ: основные подходы, основные этапы процесса.
11. Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
12. Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).
13. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
14. Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
15. Система инженерно-технической защиты информации.
16. Внедрение процессов управления ИБ: этапы и последовательность.
17. Ввод СУИБ в эксплуатацию: возможные проблемы и способы их решения.
18. Организационная основа системы обеспечения информационной безопасности РФ.
19. Основные функции системы обеспечения информационной безопасности

6.3.Вопросы к экзамену по дисциплине «Защита электронного документооборота»

1. Понятие информационной безопасности. Принципы, подходы и виды управления.
2. Цели и задачи управления ИБ. Понятие системы управления.
3. Понятие Иь. Место ИБ в рамках общей системы управления предприятием.
4. Составляющие Иь. Типовые меры по защите информации.
5. Понятие Политики СУИБ. Цели Политики СУИБ. Структура и содержание Политики СУИБ.

6. Нормативные документы в области ИБ. Законодательные и нормативно-правовые акты Российской Федерации по защите информации.
7. Структура, задачи и основные функции Государственной системы защиты информации.
8. Структура и задачи органов обеспечивающих ИБ.
9. Органы обеспечения информационной безопасности. Сертификация. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования).
10. Этапы сертификационного аудита. Решение о сертификации.
11. Эксплуатация и независимый аудит СУИБ. Методология проверки и оценки состояния информационной безопасности (защиты информации (данных) и ресурсов ИС).
12. Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация.
13. ИБ: конфиденциальность, целостность, доступность. Определения и сущность конфиденциальности, целостности, доступности- неотъемлемых составляющих информационной безопасности.
14. Организационно-технические и режимные меры и методы ИБ. Классификация и рассмотрение различных методов обеспечения информационной безопасности.
15. Обеспечение соответствия требованиям законодательства РФ. Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ (авторское право, защита персональных данных и т.д.
16. Существующие стандарты и методологии по управлению ИБ.
17. Составляющие ИБ. Разработка и управление политикой ИБ информационной системы
18. Нормативные документы в области ИБ. Анализ модели угроз ИБ и уязвимостей. Анализ модели информационных потоков.
19. Структура и задачи органов обеспечивающих ИБ. Процессы улучшения СУИБ.
20. Эксплуатация и независимый аудит СУИБ. Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Этапы сертификационного аудита. Решение о сертификации
21. ИБ: конфиденциальность, целостность, доступность.
22. Обеспечение соответствия требованиям законодательства РФ.
23. Обеспечение информационной безопасности: содержание и структура понятия.
24. Информация, защищаемая информация, объект информатизации, информационные ресурсы, информационная технология.
25. Защита информации. Основные термины и определения.
26. Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему).
27. Модели угроз и нарушителей информационной безопасности.
28. Политика ИБ и политика СУИБ: сходства и различия.
29. Внутренние аудиты ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
30. Основные функции системы обеспечения информационной безопасности

7.Учебно –методическое и информационное обеспечение дисциплины(модуля) «Защита электронного документооборота»

Зав. библиотекой

№	Виды занятий (лк, пр, лб, сре)	Комплект необходимой учебной лит-ры по дисциплинам (наименование учебника, пособия)	Авторы	Издат-во и год издания	Кол-во пособий, учебников и прочей литер-ры	
					в библ	на каф
ОСНОВНАЯ ЛИТЕРАТУРА						
1.	Лк,пз,сре	Организационное обеспечение информационной безопасности	Романов О.А., Бабин С.А., Жданов С.Г.	М.: Академия, 2008 г. — 192 стр.	7	-
2.	Лк,пз,сре	Правовое обеспечение информационной безопасности	Минаев В.А., Фисун А.П.	Москва, 2008 г. 368 с.	5	-
3.	Лк,пз,сре	Гуманитарные аспекты информационной безопасности [Электронный ресурс]: методология и методика поиска истины, построения доказательств и защиты от манипуляций	Э. П. Генлов, Ю. А. Гатчин, А. П. Пырков, В. В. Сухостат.	СПб.: Университет ИТМО, 2016. — 123 с. — 2227-8397.		http://www.iprbookshop.ru/66436.html
4.	Лк,пз,сре	Гуманитарные аспекты информационной безопасности [Электронный ресурс] : основные понятия, логические основы и операции	Э. П. Генлов, Ю. А. Гатчин, А. П. Пырков [и др.]	СПб. : Университет ИТМО, 2016. — 124 с. — 2227-8397. —		http://www.iprbookshop.ru/66435.html
ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА						
5.	Лк,пз,сре	Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект [Электронный ресурс]: учебное пособие	А. П. Кубанков, И. И. Куняев ; под ред. А. В. Морозов.	М.: Всероссийский государственный университет юстиции (РПА Минюста России), 2014. — 78 с. — 978-5-89172-850-9.		http://www.iprbookshop.ru/47262.html
6.	Лк,пз,сре	Нормативно-правовые аспекты обеспечения информационной безопасности инфокоммуникационных сетей [Электронный ресурс]: учебное пособие	А. С. Кремер	М.: Московский технический университет связи и информатики, 2007. 97 с. — 2227-8397		http://www.iprbookshop.ru/61745.html

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины	
7.	Научная библиотека // Российский государственный гуманитарный университет [Электронный ресурс]. – Электрон.дан. – М., cop. 1996–2018. / URL:http://www.rsuh.ru/section.html?id=677.
8.	Официальный сайт Министерства образования и науки РФ./ URL:- http://минобрнауки.рф/
9.	Научная электронная библиотека «КИБЕРЛЕНИНКА» URL:http://cyberleninka.ru/

8.Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий на факультете имеется комплект технических средств обучения в составе:

- интерактивная доска;

–переносной компьютер;

проектор (разрешение не менее 1280х1024);

Для проведения лабораторных занятий имеется компьютерный класс, оборудованный компьютерами с установленным программным обеспечением, предусмотренным программой дисциплины.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.03- «Информационная безопасность автоматизированных систем, специализация «Безопасность открытых информационных систем».

Рецензент от выпускающей кафедры (работодателя) по специальности _____ подпись З.Р. Рагимова ФИО

Дополнения и изменения в рабочей программе
на 20 / учебный год

В рабочую программу вносятся следующие изменения:

Рабочая программа пересмотрена на заседании кафедры 20

Заведующий кафедрой

Декан
Проректор
по учебной работе