МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
Проф. Д.А. Таюрский
_____ «___»_____20__г.

подписано электронно-цифровой подписью

Программа дисциплины

Организационное и правовое обеспечение информационной безопасности

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность компьютерных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2016

Содержание

Программу дисциплины разработал(а)(и) Ситников С.Ю.

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО

Обучающийся, освоивший дисциплину (модуль), должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-5	способность использовать нормативные правовые акты в профессиональной деятельности
ПК-15	способность организовать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
ПК-8	способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

Знать:

нормативно-правовые основы и документы по проблеме организационного обеспе-чения информационной безопасности, основные составляющие проблемы и концептуальные положения, угрозы информационной безопасности и меры защиты и противодей-ствия, основные мероприятия по созданию и обеспечению функционирования комплекс-ной системы защиты; требования и рекомендации по защите информации и требования по технической защите информации.

Должен уметь:

Уметь:

использовать нормативно-правовую базу в решении задач обеспечения информаци-онной безопасности и комплексной защиты информации на предприятии и в организации; строить концептуальные модели информационной безопасности объекта, формули-ровать основные задачи по созданию и обеспечению функционирования комплексной системы защиты на предприятии, в организации.

Должен владеть:

Владеть:

навыками работы с нормативно-правовыми и организационно-распорядительными документами в сфере информационной безопасности, вопросами технологии подбора сотрудников и работы с кадрами с точки зрения обеспечения информационной безопасности, основами организации внутриобъектового режима.

Должен демонстрировать способность и готовность:

Знать:

нормативно-правовые основы и документы по проблеме организационного обеспечения информационной безопасности, основные составляющие проблемы и концептуальные положения, угрозы информационной безопасности и меры защиты и противодействия, основные мероприятия по созданию и обеспечению функционирования комплекс-ной системы защиты; требования и рекомендации по защите информации и требования по технической защите информации.

Уметь:

использовать нормативно-правовую базу в решении задач обеспечения информационной безопасности и комплексной защиты информации на предприятии и в организации; строить концептуальные модели информационной безопасности объекта, формулировать основные задачи по созданию и обеспечению функционирования комплексной системы защиты на предприятии, в организации.

Владеть:

навыками работы с нормативно-правовыми и организационно-распорядительными документами в сфере информационной безопасности, вопросами технологии подбора сотрудников и работы с кадрами с точки зрения обеспечения информационной безопасности, основами организации внутриобъектового режима.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.Б.11 Дисциплины (модули)" основной профессиональной образовательной программы 10.03.01 "Информационная безопасность (Безопасность компьютерных систем)" и относится к базовой (общепрофессиональной) части.
Осваивается на 2 курсе в 4 семестре.

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

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) на 108 часа(ов).

Контактная работа - 54 часа(ов), в том числе лекции - 36 часа(ов), практические занятия - 18 часа(ов), лабораторные работы - 0 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 54 часа(ов).

Контроль (зачёт / экзамен) - 0 часа(ов).

Форма промежуточного контроля дисциплины: зачет в 4 семестре.

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

4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Методы, проблемы, стратегии и уровни информационной безопасности	4	4	2	0	6
2.	Тема 2. Концептуальные положения организационного обеспечения ИБ	4	4	2	0	6
3.	Тема 3. Информационная безопасность на объекте	4	4	2	0	6
4.	Тема 4. Конфиденциальная информация	4	4	2	0	6
5.	Тема 5. Организационная структура и основные мероприятия по созданию и обеспечению функционирования комплексной системы ЗИ	4	4	2	0	6
6.	Тема 6. Система организационно-распорядительных документов по организации комплексной системы ЗИ	4	4	2	0	6
7.	Тема 7. Разработка технико-экономического обоснования создания СФЗ и комплекса ИТСО	4	4	2	0	6
8.	Тема 8. Технологии защиты от угроз экономической безопасности	4	4	2	0	6
9.	Тема 9. Требования и рекомендации по защите информации	4	4	2	0	6
	Итого		36	18	0	54

4.2 Содержание дисциплины (модуля)

Тема 1. Методы, проблемы, стратегии и уровни информационной безопасности

1.1 Задачи и методы комплексного обеспечения ИБ. Содержание основных используемых в ИБ понятий. Определение защиты информации. Основные методы обеспечения ИБ.

1.2 Проблема ИБ. Определение ИБ. Актуальные проблемы создания и совершенствования системы ЗИ. Элементы эффективной и гибкой системы управления региональной системы ЗИ и основные вопросы, решаемые при её создании. Два вида проблем.

1.3. Основные составляющие ИБ. Категории спектра интересов, связанных с использованием инф. си-стем. Понятия доступности, целостности и конфиденциальности, их смысл в контексте проблемы ИБ.

Тема 2. Концептуальные положения организационного обеспечения ИБ

2.1. Общие сведения о доктрине и концепции организационного обеспечения безопасности. Цель и область применения концепции. Основания и исходные данные для разработки концепции.

2.2. Задачи обеспечения национальной безопасности в информационной сфере. Наиболее значимые задачи в гуманитарной области и в области обеспечения безопасности информационной инфраструктуры и ресурсов.

Тема 3. Информационная безопасность на объекте

3.1 Угрозы ИБ на объекте. Источники угроз безопасности. Деление источников угроз на группы, субъекты угроз. Виды угроз безопасности, классификация. Дополнительное деление на внутренние и внешние угрозы. Каналы утечки информации.

3.2 Модель угроз безопасности на объекте. Методы защиты. Основные группы методов (способов) за-щиты информации. Основные уровни защиты. 3.3 Принципы комплексной защиты информации. Основные принци-пы. Расшифровка понятий.

3.4 Система обеспечения ИБ, общие сведения об ИТКС. Стадии создания системы обеспечения безопасности. Организационные и технические мероприятия на каждой из стадий. Мероприятия, проводимые в процессе эксплуатации ИТКС. Понятие необходимого уровня защиты.

3.5. Предпосылки появления угроз в ИТКС, их возможные разновидности, интерпретация. Определение угрозы ИБ в ИТКС. Существующие классификации угроз и их источников в ИТКС.

3.6. Критерии деления множества угроз в ИТКС на классы. Наиболее опасные угрозы ИБ в ИТКС. Воздействия нарушителя на систему на различных этапах функционирования ИТКС, направления воздействия.

Тема 4. Конфиденциальная информация

4.1. Организация службы безопасности объекта. Отношения объекта и субъекта в информационном процессе с противоположными интересами с позиции активности в действиях. Определение понятия утечки информации. Уязвимые места в ИБ. Признаки наличия уязвимых мест. Примеры, способствующие неправомерному овладению конфиденциальной информацией. Каналы, способы и средства. Формы и методы недобросовестной конкуренции в контексте проблемы защиты информации. Совокупность определений, способов и средств НСД к информации на объекте. 4.2. Направления обеспечения ИБ на объекте. Номативно-правовые категории. Направления обеспечения безопасности и защиты информации. Защитные действия и их характеристики. Средства и методы организационной защиты. Определение организационной защиты. Состав мероприятий организационной защиты. 4.3. Специальные штатные службы и структуры ЗИ. Служба безопасности предприятия, её структурные единицы. Задачи службы безопасности предприятия. 4.4. Концепция создания физической защиты важных объектов. Основные термины и определения. Система физической защиты, определение. Деление СФЗ на подсистемы. Стадии проектирования объектов защиты. Основные этапы стадии концептуального проекта. Концепция физической безопасности объекта. Основные вопросы концепции: предметы защиты, угрозы безопасности и модель вероятных исполнителей угроз, оценка и анализ уязвимости и общие рекомендации по обеспечению безопасности объекта. Меры физической безопасности.

Тема 5. Организационная структура и основные мероприятия по созданию и обеспечению функционирования комплексной системы ЗИ

5.1. Цели, задачи и субъекты ИБ. Основные цели и задачи обеспечения ИБ. Управление ИБ. Классификация субъектов, влияющих на состояние ИБ.

5.2. Организационная структура системы обеспечения ИБ. Регламентация действий пользователей и обслуживающего персонала АС. Служба (подразделение) ЗИ. Уровни организационной структуры системы обеспечения ИБ АС организации. Технология обеспечения ИБ.

Тема 6. Система организационно-распорядительных документов по организации комплексной системы ЗИ

6.1. Концепция обеспечения ИБ на предприятии. Концепция обеспечения ИБ организации

Основные принципы формирования перечня критичных ресурсов, нуждающихся в защите, формируемого в процессе проведения аудита безопасности и анализа рисков. Данный перечень должен включать в себя описание физических, программных и информационных ресурсов с определением стоимости ресурсов и степени их критичности для предприятия.

Основные принципы защиты, определяющие стратегию обеспечения информационной безопасности (ИБ) и перечень правил, которыми необходимо руководствоваться при построении системы обеспечения информационной безопасности (СОИБ) предприятия.

Модель нарушителя безопасности, определяемую на основе обследования ресурсов системы и способов их использования.

Модель угроз безопасности и оценку рисков, связанных с их осуществлением, формируемую на основе перечня критичных ресурсов и модели нарушителя, которая включает определение вероятностей угроз и способов их осуществления, а также оценку возможного ущерба.

Требования безопасности, определяемые по результатам анализа рисков.

Меры обеспечения безопасности организационного и программно-технического уровня, предпринимаемые для реализации перечисленных требований.

Ответственность сотрудников предприятия за соблюдение установленных требований ИБ при эксплуатации информационной системы (ИС) предприятия.

Тема 7. Разработка технико-экономического обоснования создания СФЗ и комплекса ИТСО

7.1. Задачи концептуального проектирования. Концептуальный проект. Оценка эффективности вариантов.

7.2. Создание службы безопасности организации. Разрешенные виды деятельности Службы безопасности. Организация службы экономической безопасности. Этапы, рекомендуемые при создании Службы экономической безопасности.

Тема 8. Технологии защиты от угроз экономической безопасности

8.1. Общий алгоритм действий и активная модель реагирования. Последовательность операций (действий). Система предупредительных мер. Нестандартные угрозы. Активная модель реагирования.

8.2. Предупредительная работа с персоналом. Индикаторы выявления. Потенциальные нарушители. Проверки персонала, некоторые способы.

Тема 9. Требования и рекомендации по защите информации

10.1. Требования по технической защите информации. Организация охраны объектов.

11.1. Организационно-пропускной режим на предприятии.

11.2. Подготовка исходных данных.

11.3. Оборудование пропускных пунктов.

11.4. Организация пропускного режима. Система защиты информации и ее задачи.

12.1. Организационная система защиты информации. Государственная политика и общее руководство деятельностью по защите информации.

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

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства образования и науки Российской Федерации от 5 апреля 2017 года №301)

Письмо Министерства образования Российской Федерации №14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Устав федерального государственного автономного образовательного учреждения "Казанский (Приволжский) федеральный университет"

Правила внутреннего распорядка федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"

Локальные нормативные акты Казанского (Приволжского) федерального университета

6. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств по дисциплине (модулю) включает оценочные материалы, направленные на проверку освоения компетенций, в том числе знаний, умений и навыков. Фонд оценочных средств включает оценочные средства текущего контроля и оценочные средства промежуточной аттестации.

В фонде оценочных средств содержится следующая информация:

- соответствие компетенций планируемым результатам обучения по дисциплине (модулю);

- критерии оценивания сформированности компетенций;

- механизм формирования оценки по дисциплине (модулю);
- описание порядка применения и процедуры оценивания для каждого оценочного средства;
- критерии оценивания для каждого оценочного средства;
- содержание оценочных средств, включая требования, предъявляемые к действиям обучающихся, демонстрируемым результатам, задания различных типов.

Фонд оценочных средств по дисциплине находится в Приложении 1 к программе дисциплины (модулю).

7. Перечень литературы, необходимой для освоения дисциплины (модуля)

Освоение дисциплины (модуля) предполагает изучение основной и дополнительной учебной литературы. Литература может быть доступна обучающимся в одном из двух вариантов (либо в обоих из них):

- в электронном виде - через электронные библиотечные системы на основании заключенных КФУ договоров с правообладателями;
- в печатном виде - в Научной библиотеке им. Н.И. Лобачевского. Обучающиеся получают учебную литературу на абонементе по читательским билетам в соответствии с правилами пользования Научной библиотекой.

Электронные издания доступны дистанционно из любой точки при введении обучающимся своего логина и пароля от личного кабинета в системе "Электронный университет". При использовании печатных изданий библиотечный фонд должен быть укомплектован ими из расчета не менее 0,5 экземпляра (для обучающихся по ФГОС 3++ - не менее 0,25 экземпляра) каждого из изданий основной литературы и не менее 0,25 экземпляра дополнительной литературы на каждого обучающегося из числа лиц, одновременно осваивающих данную дисциплину.

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля), находится в Приложении 2 к рабочей программе дисциплины. Он подлежит обновлению при изменении условий договоров КФУ с правообладателями электронных изданий и при изменении комплектования фондов Научной библиотеки КФУ.

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Гарант - http://www.garant.ru/

Консультант Плюс - http://www.consultant.ru/

Официальный портал правовой информации - http://pravo.gov.ru/

Российская газета - http://www.rg.ru/

Собрание законодательства РФ - http://www.szrf.ru/

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид работ	Методические рекомендации
лекции	Структура лекции 1. Инструктивный блок (продолжительность около 5 мин.) его задача ? дать студентам всю возможную информацию о порядке изучения темы. 1.1. Слайд с вопросами лекции. Объяснение преподавателя о цели и задачах лекции. Обоснование актуальности и практической значимости темы. Ссылки на литературу. 1.2. Интерактивный элемент. Решение управленческой задачи. Цель ? раскрепощение и активизация познавательной деятельности студентов, пробуждение интереса к рассматриваемой тематике. Методика: На слайде дано условие задачи. Студенты предлагают свои варианты решения и коллективно обсуждают результаты предложенных вариантов. Преподаватель комментирует обсуждение, побуждает аудиторию найти правильное решение задачи. 2. Информационный блок (продолжительность около 60 мин.) Основная цель ? дать студентам знания, используя максимально возможные средства передачи информации, соблюдая особенности методического и дидактического сопровождения интерактивного занятия. 2.1. Лекция-визуализация с объяснением теории ?Информационная безопасность? 2.2. Интерактивный элемент. Проработка правил безопасной работы в сети Интернет. Методика: Студентам раздаются карточки из которых они должны составит правила работы в сети Интернет с учетом законодательства. Задача: Проверка результатов задания. Правильный ответ выводится на слайд. Обсуждение ситуации. 3. Диагностический блок (продолжительность около 10 мин.). Позволяет оценить уровень развитости компетенций студентов. 3.1. Интерактивный элемент. Решение тестовых заданий. Цель: закрепление теоретического материала, рейтинговая оценка степени усвоения знаний. Методика: На экран выводятся тестовые задания, студенты отвечают на вопросы. Преподаватель организует дискуссию. Идет групповое обсуждение ответа. После обсуждения преподаватель выделяет на слайде правильный вариант ответа. Если ответ студентов был неправильным, либо они затруднились с ответом, преподаватель поясняет, почему на данный вопрос надо отвечать именно так. 4. Коммуникативный блок (продолжительность около 5 мин.) 4.1. Ответы на вопросы студентов по теме лекции.
практические занятия	Практическое задание. Интернет называют "миром новых возможностей". но тем, кто пришёл в него, следует вести себя осторожно и строго следовать правилам поведения в Сети, предусматривающими соблюдение законодательства (ст. 272 и др). Как и в реальном мире, в Интернете действует множество мошенников и просто хулиганов, которые создают и запускают вредоносные программы, нарушают приватность персональных данных, нарушают авторские права на музыкальные произведения, фильмы и т.д. Необходимо составит правила безопасной работы в Интернет. После выполнения задания. Появляется слайд с правильным ответом. Идет обсуждение.
самостоя-тельная работа	При выполнении самостоятельной работы следует следует использовать прежде всего справочную правовую систему Консультант +. Возможно использование и других справочно-информационных баз (Гарант и др.), а также официальный сайты Российской газеты. Официальный интернет-портал правовой информации http://pravo.gov.ru/

Вид работ	Методические рекомендации
зачет	Вопросы к зачету формируются из заголовков и подзаголовков разделов и подразделов лекционного материала. Пример вопросов к зачету (по два вопроса в билете). 1) Официальный источники правовой информации (Российская газета, интернет-портал http://pravo.gov.ru, собрание законодательства РФ www.szrf.ru). Правовые базы данных (Консультант+, Гарант, Кодекс, ЮСИС) 2) Положение об обеспечении безопасности персональных данных при их обработке в [автоматизированных] информационных системах персональных данных (утв. по-становлением Правительства РФ от 17 ноября 2007 г. № 781 и новый №1119) + по-становление №678 (тоже, но в неавтоматизированных ИСПДн) 3) Приказ ФСТЭК России от 5 февраля 2010 г. № 58 ?Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных? Новый приказ от 18.02.2013 №21 4) Порядок ведения персонифицированного учета в сфере обязательного медицин-ского страхования (Приказ Министерства здравоохранения и социального развития РФ от 25 января 2011 г. № 29н) 5) Объекты и субъекты авторского права. 6) Условия патентоспособности. 7) компьютерные правонарушения (ст.273 УК) + найти комментарии 8. Права и свободы гражданина и человека. 9. Концепция законодательства в сфере информационной безопасности. 10. Современного состояния информационного законодательства в РФ. 11. Воздействие "вредной" информации на индивидуальное и массовое сознание. 12. Информационно - правовое обеспечение и доступность правовой информации. 13. Информационная безопасность субъекта правовых отношений. 14. Нормативно-правовые аспекты электронного бизнеса. 15. Нормативно-правовые аспекты безопасной работы в Интернет . 16. Национальные интересы России и информационное противостояние в современ-ном мире. 17. Ценностная ориентация личности, ее информационное обоснование и информа-ционная безопасность. 18. Правовые механизмы регулирования в сфере производства и эксплуатации крип-тографических продуктов. 19. Разработка правовых механизмов регулирования электронного документообо-рота. 20. Разработка и научное обоснование путей обеспечения информационно-психологической безопасности личности и общества.

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

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем, представлен в Приложении 3 к рабочей программе дисциплины (модуля).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Материально-техническое обеспечение образовательного процесса по дисциплине (модулю) включает в себя следующие компоненты:

Помещения для самостоятельной работы обучающихся, укомплектованные специализированной мебелью (столы и стулья) и оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду КФУ.

Учебные аудитории для контактной работы с преподавателем, укомплектованные специализированной мебелью (столы и стулья).

Компьютер и принтер для распечатки раздаточных материалов.

Мультимедийная аудитория.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;

- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;

- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;

- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;

- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;

- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;

- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:

- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;

- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;

- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению 10.03.01 "Информационная безопасность" и профилю подготовки "Безопасность компьютерных систем".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.Б.11 Организационное и правовое обеспечение информационной безопасности

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность компьютерных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2016

Основная литература:

1.Ерохин В.В., Безопасность информационных систем [Электронный ресурс] / Ерохин В.В. - М. : ФЛИНТА, 2015. - 182 с. - ISBN 978-5-9765-1904-6 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785976519046.html

2. Шаньгин В.Ф., Информационная безопасность и защита информации [Электронный ресурс] / Шаньгин В.Ф. - М. : ДМК Пресс, 2014. - 702 с. - ISBN 978-5-94074-768-0 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785940747680.html

3.Новиков В.К., Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) [Электронный ресурс]: Учебное пособие. / В.К. Новиков - М. : Горячая линия - Телеком, 2015. - 176 с. - ISBN 978-5-9912-0525-2 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991205252.html

Дополнительная литература:

1.Куняев, Н. Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере [Электронный ресурс] / Н. Н. Куняев. - М.: Логос, 2010. - 348 с. - Режим доступа: http://znanium.com/bookread2.php?book=469026

2.Кузнецов, И. Н. Бизнес-безопасность [Электронный ресурс] / И. Н. Кузнецов. - 4-е изд. - М.: Дашков и К, 2016. - 416 с. - Режим доступа: http://znanium.com/bookread2.php?book=430343

3.Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс] : учеб. Пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. - Красноярск : Сиб. Гос. Аэрокосмич. Ун-т, 2012. - 100 с. - Режим доступа: http://znanium.com/bookread2.php?book=463061

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.Б.11 Организационное и правовое обеспечение информационной безопасности

Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Направление подготовки: 10.03.01 - Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2016

Освоение дисциплины (модуля) предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows 7 Профессиональная или Windows XP (Volume License)

Пакет офисного программного обеспечения Microsoft Office 365 или Microsoft Office Professional plus 2010

Браузер Mozilla Firefox

Браузер Google Chrome

Adobe Reader XI или Adobe Acrobat Reader DC

Kaspersky Endpoint Security для Windows

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.