

Департамент внутренней и кадровой политики Белгородской области
Областное государственное автономное
профессиональное образовательное учреждение
«Белгородский индустриальный колледж»

Рассмотрено
цикловой комиссией
Протокол заседания № 1
от «31» августа 2020 г.
Председатель цикловой комиссии
_____ / Чобану Л.А./

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по выполнению практических работ
учебной дисциплины
ОП. 08 Организационно-правовое обеспечение
информационной безопасности
по специальности
10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем
квалификация
техник по защите информации

Разработчик:
преподаватель
ОГАПОУ «Белгородский
индустриальный колледж»
Петрушин С.Д.

Белгород 2020 г.

Содержание

	Стр.
1. Пояснительная записка	3
1.1. Краткая характеристика дисциплины, ее цели и задачи. Место практических работ в курсе дисциплины	3
1.2. Организация и порядок проведения практических работ	3
1.3. Общие указания по выполнению практических работ	3
1.4. Критерии оценки результатов выполнения практических работ	4
2. Тематическое планирование практических работ	5
3. Содержание практических работ	6
Практическая работа №1 Проведение классификации, расследования, оформления и учёта несчастного случая в организации	6
Практическая работа №1-2 «Работа с нормативными документами»	6
Практическая работа №3-4 «Защита информации, содержащейся в информационных системах общего пользования»	8
Практическая работа №5-6 «Разработка базового блока документов для обеспечения информационной безопасности ИСПДН»	10
Практическая работа №7-8«Подготовка документов к получению лицензии»	13
Практическая работа №9-10«Подготовки документов к сертификации»	14
Практическая работа №11-12«Подготовка документов к аттестации объектов информатизации»	15
Практическая работа №13-15 «Составление трудового договора сотрудника службы информационной безопасности»	16

1. Пояснительная записка

1.1. Краткая характеристика дисциплины, ее цели и задачи. Место практических работ в курсе дисциплины

Дисциплина ОП. 08 «Организационно-правовое обеспечение информационной безопасности» является частью рабочей основной образовательной программы в соответствии с ФГОС по специальности СПО **10.02.04 Обеспечение информационной безопасности телекоммуникационных систем**

Дисциплина изучается в III-IV семестр. В целом рабочей программой предусмотрено 30 часов на выполнение практических работ, что составляет 30 % от обязательной аудиторной нагрузки, которая составляет 98 часа, при этом максимальная нагрузка составляет 102 часа, из них 4 часа приходится на самостоятельную работу обучающихся.

Цель настоящих методических рекомендаций: оказание помощи обучающимся в выполнении практических работ по дисциплине ОП. 08 «Организационно-правовое обеспечение информационной безопасности», качественное выполнение которых поможет обучающимся освоить обязательный минимум содержания дисциплины и подготовиться к промежуточной аттестации в форме диф. зачета.

1.2. Организация и порядок проведения практических работ

Практические работы проводятся после изучения теоретического материала. Введение практических работ в учебный процесс служит связующим звеном между теорией и практикой. Они необходимы для закрепления теоретических знаний, а также для получения практических навыков и умений. При проведении практических работ задания, выполняются студентом самостоятельно, с применением знаний и умений, усвоенных на предыдущих занятиях, а также с использованием необходимых пояснений, полученных от преподавателя. Обучающиеся должны иметь методические рекомендации по выполнению практических работ, конспекты лекций, измерительные и чертежные инструменты, средство для вычислений.

1.3. Общие указания по выполнению практических работ

Курс практических работ по дисциплине ОП. 08 «Организационно-правовое обеспечение информационной безопасности» предусматривает проведение 15 работ, посвященных изучению:

- работе с нормативными документами;
- защите информации, содержащейся в информационных системах общего пользования;
- разработке базового блока документов для обеспечения информационной безопасности ИСПДН;
- подготовке документов к получению лицензии;
- подготовке документов к сертификации;
- подготовке документов к аттестации объектов информатизации;
- составлению трудового договора сотрудника службы информационной безопасности.

При подготовке к проведению практической работы необходимо:

- ознакомиться с целями проведения практической работы;
- ознакомиться с порядком выполнения работы.

После выполнения практической работы обучающийся к следующему занятию оформляет отчет, который должен содержать:

- название практической работы, ее цель;
- краткие, теоретические сведения об изучаемой теме;
- все необходимые, предусмотренные практической работой, расчеты;
- выводы по итогам работы;

- ответы на контрольные вопросы.

1.4. Критерии оценки результатов выполнения практических работ

Критериями оценки результатов работы обучающихся являются:

- уровень усвоения обучающимся учебного материала;
 - умение обучающегося использовать теоретические знания при выполнении практических задач;
 - сформированность общих и профессиональных компетенций:
- ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;
- ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности;
- ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие;
- ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами;
- ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей
- ОК 09. Использовать информационные технологии в профессиональной деятельности;
- ПК 1.4. Осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей
- ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудовании информационно – телекоммуникационных систем и сетей
- ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях обоснованность и четкость изложения материала;
- уровень оформления работы.
 - анализ результатов.

Критерии оценивания практической работы

Оценка	Критерии оценивания
5	Работа выполнена в полном объеме с соблюдением необходимой последовательности проведения, содержит результаты и выводы, все записи, таблицы, рисунки, чертежи, графики выполнены аккуратно. Обучающийся владеет теоретическим материалом, формулирует собственные, самостоятельные, обоснованные, представляет полные и развернутые ответы на дополнительные вопросы.
4	Работа выполнена в полном объеме с соблюдением необходимой последовательности проведения, содержит результаты и выводы, все записи, таблицы, рисунки, чертежи, графики выполнены аккуратно. Обучающийся владеет теоретическим материалом, допуская незначительные ошибки на дополнительные вопросы.
3	Работа выполнена в полном объеме, содержит результаты и выводы, все записи, таблицы, рисунки, чертежи, графики выполнены аккуратно. Обучающийся владеет теоретическим материалом на минимально допустимом уровне, допуская ошибки на дополнительные вопросы.
2	Работа выполнена не полностью. Студент практически не владеет теоретическим материалом, допускает ошибки при ответе на дополнительные вопросы.

2. Тематическое планирование практических работ

	Наименование тем	Вид и название работы студента	Количество часов на выполнение работы
Раздел 1	Правовое обеспечение информационной безопасности		12
1.3.	Информация как объект правового регулирования	Практическая работа №1-2 «Работа с нормативными документами»	4
		Практическая работа №3-4 «Защита информации, содержащейся в информационных системах общего пользования»	4
1.5.	Правовые режимы защиты конфиденциальной информации	Практическая работа №5-6 «Разработка базового блока документов для обеспечения информационной безопасности ИСПДН»	4
Раздел 2	Лицензирование и сертификация в области защиты информации		12
2.1.	Лицензирование деятельности в области защиты информации	Практическая работа №7-8 «Подготовка документов к получению лицензии»	4
2.2.	Сертификация и аттестация по требованиям безопасности информации	Практическая работа №9-10 «Подготовки документов к сертификации»	4
		Практическая работа №11-12 «Подготовка документов к аттестации объектов информатизации»	4
Раздел 4.	Основы трудового права		6
4.1.	Законодательные и нормативные правовые акты, регламентирующие трудовые правоотношения	Практическая работа №13-15 «Составление трудового договора сотрудника службы информационной безопасности»	6
		Итого:	30

3. Содержание практических работ ПРАКТИЧЕСКАЯ РАБОТА № 1-2 РАБОТА С НОРМАТИВНЫМИ ДОКУМЕНТАМИ

Цель: ознакомиться и получить практические навыки работы со справочной правовой системой на примере справочной системы «КонсультантПлюс».

Теоретические вопросы

1. Объясните назначение справочных систем типа «КонсультантПлюс».
2. Перечислите компоненты меню стартовой страницы.
3. В чем заключается польза путеводителей? Какой из путеводителей вы будете использовать при ведении поиска информации, связанной с информационной безопасностью?
4. Что такое карточка поиска?
5. В каких случаях используется совместная работа быстрого поиска и правового навигатора?
6. Опишите поиск фрагмента текста.
7. Расскажите о назначении «умных ссылок».
8. Перечислите ряд первоочередных мер по предотвращению угроз национальным интересам.
9. Какие вы можете назвать способы сохранения собранной информации?
10. Для каких целей используются закладки?
11. Поясните принцип работы истории поисков.

Задание 1. Используя «Руководство пользователя» (РК) по работе со справочной правовой системой «КонсультантПлюс», познакомиться со структурой интерфейса программы, процессами запуска системы, назначением вкладок.

Задание 2. Найти ФЗ-152.

Задание 3. Найти статьи УК РФ, относящиеся к правонарушениям в сфере информационных технологий.

Задание 4. Определите дату принятия Доктрины информационной безопасности РФ.

Задание 5. Найти информацию о наказании за разработку вредоносного программного обеспечения.

Задание 6. Найти последний законодательный акт, принятый в сфере информационной безопасности.

Задание 7. Найти статью «Правовая защита цифрового контента от пиратства в сети Интернет и ее влияние на развитие телевизионной и киноотрасли».

Задание 8. Провести сравнение редакций закона «О связи».

Задание 9. Найти форму приказа на увольнение.

Литература

Основные источники

1. Пржегорлинский, В. Н. Организационно-правовое обеспечение информационной безопасности. - М.: Академия, 2018.

Дополнительные источники

1. Бубнов, А. А., Пржегорлинский, В.Н., Савинкин, О.А. Основы информационной безопасности. - М.: Академия. 2016.

2. Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности. - СПб.: НИУ ИТМО, 2016.
3. Кармановский, Н. С. и др. Организационно-правовое и методическое обеспечение информационной безопасности. - Учебное пособие. — СПб.: НИУ ИТМО. — 2016.
4. Организационно-правовое обеспечение информационной безопасности: учеб. Пособие для студентов вузов / под ред. А. А. Стрельцова. - М.: Изд. Центр «Академия»
5. Родичев, Ю. А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. - СПб.: Изд. Питер. 2017.

ПРАКТИЧЕСКАЯ РАБОТА № 3-4
ЗАЩИТА ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОБЩЕГО ПОЛЬЗОВАНИЯ

Цель: защита информации, содержащейся в информационных системах общего пользования.

Теоретические вопросы

1. Основания защиты информации в информационной системе.
2. Классификация информационной системы по требованиям защиты информации.
3. Определение актуальных угроз безопасности информации и разработка модели угроз безопасности информации.
4. Разработка системы защиты информации.
5. Разработка эксплуатационной документации на систему защиты информации.
6. Требования к мерам защиты информации.
7. Система защиты информации на предприятии.

Задание 1. Проведите анализ специальных понятий: «социальная информация»,

«документальная информация», «правовая информация», «научная информация» и приведите примеры информации, которая может быть отнесена к данным понятиям.

Задание 2. Определите, к какому виду информации в зависимости от порядка ее предоставления или распространения относится информация в конкретных ситуациях:

а) юридическое лицо заключило с таможенным представителем договор представлять свои интересы при оформлении таможенной декларации и помещении товаров под определённую таможенную процедуру, при перемещении товаров через таможенную границу Таможенного союза, и предоставил ему информацию о себе, товаре и его назначении;

б) государственный фонд данных государственного экологического мониторинга (государственного мониторинга окружающей среды) включает в себя:

- информацию, содержащуюся в базах данных подсистем единой системы государственного экологического мониторинга (государственного мониторинга окружающей среды);

- результаты производственного контроля в области охраны окружающей среды и государственного экологического надзора;

- данные государственного учета объектов, оказывающих негативное воздействие на окружающую среду;

в) при принятии бюджета на 2017 год и плановый период на 2018-2019 годы Комитет Государственной Думы по бюджетному планированию рассмотрел источник доходов и размеры финансирования на обеспечения обороноспособности страны с подробным указанием всех статей расходов.

Задание 3. Доступ на территорию организации осуществляется через пост вневедомственной охраны с проходом через турникет и фиксацией времени входа-выхода сотрудников. Посетители проходят по пропускам при предъявлении документа, удостоверяющего личность. Однако это не регламентировано никаким документом, с которым под роспись ознакомлены ответственные должностные лица, а также не определены мероприятия по контролю соблюдения установленных требований.

Как вы считаете, приняты ли все организационные меры, направленные на физическую защиту объекта в данной организации?

Задание 4. Разработать систему защиты информации в информационной системе на предприятии (выбор системы и предприятия произвольно), содержащую следующие основные пункты:

- проблемная ситуация в сфере информационной безопасности;
- механизмы обеспечения информационной безопасности предприятия;
- мероприятия по реализации мер информационной безопасности предприятия;
- программа создания системы информационной безопасности предприятия.

Задание 5. Проанализируйте Доктрину информационной безопасности Российской Федерации, утвержденной Президентом РФ от 5 декабря 2016 г. № 646 и определите основные направления обеспечения информационной безопасности в экономической сфере России.

Литература

Основные источники

1. Пржегорлинский, В. Н. Организационно-правовое обеспечение информационной безопасности. - М.: Академия, 2018.

Дополнительные источники

1. Бубнов, А. А., Пржегорлинский, В.Н., Савинкин, О.А. Основы информационной безопасности. - М.: Академия. 2016.

2. Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности. - СПб.: НИУ ИТМО, 2016.

3. Кармановский, Н. С. и др. Организационно-правовое и методическое обеспечение информационной безопасности. - Учебное пособие. — СПб.: НИУ ИТМО. — 2016.

4. Организационно-правовое обеспечение информационной безопасности: учеб. Пособие для студентов вузов / под ред. А. А. Стрельцова. - М.: Изд. Центр «Академия»

5. Родичев, Ю. А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. - СПб.: Изд. Питер. 2017

ПРАКТИЧЕСКАЯ РАБОТА № 5-6
РАЗРАБОТКА БАЗОВОГО БЛОКА ДОКУМЕНТОВ ДЛЯ ОБЕСПЕЧЕНИЯ ИН-
ФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИСПДН

Цель: разработка базового блока документов для обеспечения информационной безопасности ИСПДн.

Теоретические вопросы

1. Становление и развитие института персональных данных в Российской Федерации.
2. Понятие и виды персональных данных.
3. Защита персональных данных.
4. Особенности защиты персональных данных в трудовых отношениях.
5. Особенности защиты персональных данных в сети Интернет.
6. Порядок ограничения доступа к информации, обрабатываемой с нарушением законодательства РФ в области персональных данных.
7. Обеспечение записи, систематизации, накопления, хранения, уточнения, извлечения персональных данных граждан РФ с использованием баз данных, находящихся на территории РФ.
8. Органы по защите прав субъектов персональных данных.
9. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника.

Задание 1. Изучите закон «О персональных данных».

Задание 2. Мировой судья направил запрос о состоянии здоровья в больницу, где проходил лечение гражданин Т., в отношении которого судьёй проводится расследование и получил из больницы сведения, составляющие врачебную тайну. Согласие гражданина Т. на разглашение врачебной тайны не получали.

Соответствует ли данная ситуация законодательству о персональных данных? Имеет ли право мировой судья передавать эти сведения адвокату гражданина Т.?

Задание 3. Гражданин Воронов подозревался в совершении преступления. В отношении него в пределах, допускаемых требованиями конспирации, были осуществлены оперативно-разыскные действия и собрана о нем информация, в том числе о его личной жизни. Однако виновность Воронова в совершении преступления не доказана и в отношении него в возбуждении уголовного дела отказано.

Так как Воронов располагает фактами проведения в отношении него оперативно-разыскных мероприятий и полагает, что при этом были нарушены его права, вправе ли он потребовать сведения о полученной информации о нем?

Задание 4. Какие сведения предоставляются средствам массовой информации по их обращениям о персональных данных государственного гражданского служащего Российской Федерации? Какие ограничения, связанные с обеспечением частной жизни публичных персон, установлены в современном законодательстве?

Задание 5. Как вы объясните требование представить медицинскую справку о состоянии здоровья при поступлении на работу в детский сад, продовольственные отделы магазинов. Какой вид персональных данных составляют эти персональные данные?

Задание 6. Если банк обращается в организацию с целью проверки сведений о лице, обратившемся за кредитом с вопросами: работает ли данное лицо в этой организации, какой

имеет размер зарплаты и т.п., обязана ли организация предоставить в банк данную информацию о работнике.

Задание 7. Создайте или найдите в сети Интернет и адаптируйте под свою организацию следующие документы:

- «Согласие на обработку персональных данных»;
- «Отзыв согласия на обработку персональных данных».

Задание 8. Сравните понятия «частная жизнь», «персональные данные», «конфиденциальная информация» в аспекте трудового права.

Задание 9. При проведении проверки первичной документации по учёту труда и его оплаты было обнаружено, что в личном деле одного из референтов федерального агентства отсутствуют сведения из налоговой службы об имущественном положении, а также данные дактилоскопической регистрации. Инспектор труда потребовал предъявить указанные документы.

Правомерны ли требования инспектора труда?

Задание 10. Начальник отдела кадров Дубовцева распространяла среди своих знакомых сведения об образовании и данные медицинского осмотра заведующего складом Мамонтова, которые, по её мнению, порочили его честь и достоинство. Мамонтов потребовал от директора организации защитить его персональные данные от неправомерного использования и привлечь Дубовцеву к административной ответственности. Директор оштрафовал Дубовцеву на сумму, равную трем минимальным размера оплаты труда.

Законно ли действие работодателя? Какие виды юридической ответственности установлены законодательством России за нарушение норм, регулирующих сбор, обработку, хранение, распространение и защиту персональных данных работника.

Задание 11. В ОАО «Решение» было разработано и утверждено приказом директора Положение о порядке обработки и хранения персональных данных работников. Директор поручил своему заместителю ознакомить с положением всех работников под расписку.

Правомерно ли действие директора ОАО? Кто по законодательству имеет право вырабатывать меры защиты персональных данных работников, порядок их сбора, хранения и использования?

Задание 12. Перевалов обратился в центр занятости по месту жительства в целях поиска подходящей работы. Инспектор центра занятости потребовал от гражданина предоставить сведения о последнем месте работы, о составе его семьи, его религиозных убеждениях и принадлежности к политическим партиям. Считая такие требования незаконными, Перевалов обратился с жалобой к руководителю центра занятости.

Законны ли требования инспектора. Какое решение по жалобе должен принять руководитель центра занятости?

Задание 13. Составьте проект:

- дополнительного соглашения к трудовому договору об изменении персональных данных работника;
- запроса о предоставлении персональных данных работника;
- положения о персональных данных работников организации.

Литература
Основные источники

1. Пржегорлинский, В. Н. Организационно-правовое обеспечение информационной безопасности. - М.: Академия, 2018.

Дополнительные источники

1. Бубнов, А. А., Пржегорлинский, В.Н., Савинкин, О.А. Основы информационной безопасности. - М.: Академия. 2016.

2. Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности. - СПб.: НИУ ИТМО, 2016.

1. Кармановский, Н. С. и др. Организационно-правовое и методическое обеспечение информационной безопасности. - Учебное пособие. — СПб.: НИУ ИТМО. — 2016.

2. Организационно-правовое обеспечение информационной безопасности: учеб. Пособие для студентов вузов / под ред. А. А. Стрельцова. - М.: Изд. Центр «Академия»

3. Родичев, Ю. А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. - СПб.: Изд. Питер. 2017

ПРАКТИЧЕСКАЯ РАБОТА № 7-8

ПОДГОТОВКА ДОКУМЕНТОВ К ПОЛУЧЕНИЮ ЛИЦЕНЗИИ

Цель: подготовка документов к получению лицензии.

Теоретические вопросы

1. Организационная структура системы государственного лицензирования в области защиты информации.
2. Общий порядок проведения лицензирования в области защиты информации.
3. Контроль за деятельностью лицензиатов.
4. Изучение перечня видов деятельности предприятий в области защиты информации, подлежащих лицензированию.
5. Функции государственных органов по лицензированию в области защиты информации.
6. Назовите случаи приостановления или прекращения действия лицензии.

Задание 1. Используя справочно-правовые системы ознакомиться с нормативно-правовыми актами, регулирующими лицензирование отдельных видов предпринимательской деятельности.

Задание 2. Используя открытые источники, в том числе интернет-источники, выяснить расценки на лицензии конкретных видов деятельности.

Задание 3. Составить заявление о предоставлении лицензии на деятельность по технической защите конфиденциальной информации юридическому лицу.

Литература

Основные источники

1. Пржегорлинский, В. Н. Организационно-правовое обеспечение информационной безопасности. - М.: Академия, 2018.

Дополнительные источники

1. Бубнов, А. А., Пржегорлинский, В.Н., Савинкин, О.А. Основы информационной безопасности. - М.: Академия. 2016.
2. Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности. - СПб.: НИУ ИТМО, 2016.
3. Кармановский, Н. С. и др. Организационно-правовое и методическое обеспечение информационной безопасности. - Учебное пособие. — СПб.: НИУ ИТМО. — 2016.
4. Организационно-правовое обеспечение информационной безопасности: учеб. Пособие для студентов вузов / под ред. А. А. Стрельцова. - М.: Изд. Центр «Академия»
5. Родичев, Ю. А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. - СПб.: Изд. Питер. 2017

ПРАКТИЧЕСКАЯ РАБОТА № 9-10 ПОДГОТОВКИ ДОКУМЕНТОВ К СЕРТИФИКАЦИИ

Цель: подготовка документов к сертификации.

Теоретические вопросы

1. Система сертификации средств защиты информации по требованиям безопасности информации.
2. Организационная структура системы сертификации средств защиты информации по требованиям безопасности информации.
3. Виды и схемы сертификации средств защиты информации.
4. Функции ФСТЭК в области сертификации средств защиты информации.
5. Функции органов сертификации средств защиты информации.
6. Функции испытательных лабораторий (центров).
7. Функции заявителей.
8. Порядок проведения сертификации и контроля.
9. Перечень средств защиты информации, подлежащих сертификации.

Задание 1. Сформулируйте цели системы сертификации средств защиты информации по требованиям безопасности информации.

Задание 2. Назовите виды и схемы сертификации средств защиты информации.

Задание 3. Назовите функции органов сертификации средств защиты информации.

Задание 4. Опишите общий порядок проведения сертификации средств защиты информации.

Задание 5. Составить заявление на сертификацию средства защиты информации.

Литература

Основные источники

1. Пржегорлинский, В. Н. Организационно-правовое обеспечение информационной безопасности. - М.: Академия, 2018.

Дополнительные источники

1. Бубнов, А. А., Пржегорлинский, В.Н., Савинкин, О.А. Основы информационной безопасности. - М.: Академия. 2016.

2. Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности. - СПб.: НИУ ИТМО, 2016.

3. Кармановский, Н. С. и др. Организационно-правовое и методическое обеспечение информационной безопасности. - Учебное пособие. — СПб.: НИУ ИТМО. — 2016.

4. Организационно-правовое обеспечение информационной безопасности: учеб. Пособие для студентов вузов / под ред. А. А. Стрельцова. - М.: Изд. Центр «Академия»

5. Родичев, Ю. А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. - СПб.: Изд. Питер. 2017

ПРАКТИЧЕСКАЯ РАБОТА № 11-12
ПОДГОТОВКА ДОКУМЕНТОВ К АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИ-
ЗАЦИИ

Цель: подготовка документов к аттестации объектов информатизации.

Теоретические вопросы

1. Система объектов информатизации по требованиям безопасности информации.
2. Виды аттестации объектов информатизации по требованиям безопасности информации.
3. Функции ФСТЭК и органов по аттестации в области аттестации объектов информатизации по требованиям безопасности информации.
4. Функции испытательных центров (лабораторий) и заявителей по аттестации объектов информатизации по требованиям безопасности информации.
5. Порядок проведения аттестации и контроля.

Задание 1. Приведите объекты информатизации, которые подлежат обязательной аттестации.

Задание 2. Опишите порядок проведения аттестации объектов информатизации по требованиям безопасности информации.

Задание 3. Приведите сведения, на основании которых разрабатывается программа аттестационных испытаний.

Задание 4. Перечислите сведения об объекте, представленные в техническом паспорте объекта информатизации.

Задание 5. Перечислите виды аттестации помещений по требованиям безопасности информации.

Задание 6. Ознакомьтесь с "Положением об аттестации объектов информатизации по требованиям безопасности". Составьте заявление на аттестацию объекта информатизации по требованиям безопасности.

Литература

Основные источники

1. Пржегорлинский, В. Н. Организационно-правовое обеспечение информационной безопасности. - М.: Академия, 2018.

Дополнительные источники

1. Бубнов, А. А., Пржегорлинский, В.Н., Савинкин, О.А. Основы информационной безопасности. - М.: Академия. 2016.

2. Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности. - СПб.: НИУ ИТМО, 2016.

3. Кармановский, Н. С. и др. Организационно-правовое и методическое обеспечение информационной безопасности. - Учебное пособие. — СПб.: НИУ ИТМО. — 2016.

4. Организационно-правовое обеспечение информационной безопасности: учеб. Пособие для студентов вузов / под ред. А. А. Стрельцова. - М.: Изд. Центр «Академия»

5. Родичев, Ю. А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. - СПб.: Изд. Питер. 2017.

ПРАКТИЧЕСКАЯ РАБОТА № 13-15
СОСТАВЛЕНИЕ ТРУДОВОГО ДОГОВОРА СОТРУДНИКА СЛУЖБЫ ИН-
ФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Цель: составление трудового договора сотрудника службы информационной безопасности.

Теоретические вопросы

1. Понятие трудового договора, его виды.
2. Перечень документов, предъявляемых при поступлении на работу.
3. Этапы оформления трудовых отношений.
4. Основания прекращения трудового договора.

Задание 1. Оформить документы о приеме на работу сотрудника службы информационной безопасности:

- заявление о приеме на работу;
- резюме работника;
- приказ руководителя предприятия о приеме на работу; в тексте приказа обязательно должно быть указано несколько существенных условий договора. Как правило: дата начала работы, место работы, должность, размер оплаты труда, условия об испытательном сроке, режим работы.

Задание 2. Составить и оформить трудовой договор с сотрудником службы информационной безопасности в полном соответствии с законодательством РФ.

Литература
Основные источники

1. Пржегорлинский, В. Н. Организационно-правовое обеспечение информационной безопасности. - М.: Академия, 2018.

Дополнительные источники

1. Бубнов, А. А., Пржегорлинский, В.Н., Савинкин, О.А. Основы информационной безопасности. - М.: Академия. 2016.
2. Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности. - СПб.: НИУ ИТМО, 2016.
3. Кармановский, Н. С. и др. Организационно-правовое и методическое обеспечение информационной безопасности. - Учебное пособие. — СПб.: НИУ ИТМО. — 2016.
4. Организационно-правовое обеспечение информационной безопасности: учеб. Пособие для студентов вузов / под ред. А. А. Стрельцова. - М.: Изд. Центр «Академия»
5. Родичев, Ю. А. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. - СПб.: Изд. Питер. 2017

Департамент внутренней и кадровой политики Белгородской области
Областное государственное автономное
профессиональное образовательное учреждение
«Белгородский индустриальный колледж»

Группа 21 БТС

ЖУРНАЛ ОТЧЕТОВ
по выполнению практических работ
учебной дисциплины
**ОП. 08 Организационно-правовое обеспечение информационной безопас-
ности**
по специальности
**10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем**

ВЫПОЛНИЛ _____ / _____ /

ПРИНЯЛ _____ /Рачинский С.А./

Белгород 2019 г.