Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»

УТВЕРЖДАЮ
Заместитель директора
по учебно-производственной работе
_____ О.В. Фомичева
«26» декабря 2023 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по выполнению практических работ
по учебной дисциплине
ОП.02 ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

для специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Санкт-Петербург
2023 г.

Методические рекомендации рассмотрены на заседании методического совета СПб ГБПОУ «АУГСГиП»

Протокол № 2 от «29» ноября 2023 г.

Методические рекомендации одобрены на заседании цикловой комиссии общетехнических дисциплин и компьютерных технологий

Протокол № 4 от «21» ноября 2023 г.

Председатель цикловой комиссии: Караченцева М.С. _____

Разработчики: преподаватели СПб ГБПОУ «АУГСГиП»

С О Д Е Р Ж А Н И Е

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая тетрадь по выполнению практических работ предназначены для организации работы на практических занятиях по учебной дисциплине «Организационно-правовое обеспечение информационной безопасности», которая является важной составной частью в системе подготовки специалистов среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Практические занятия являются неотъемлемым этапом изучения учебной дисциплины и проводятся с целью:

- формирования практических умений в соответствии с требованиями к уровню подготовки обучающихся, установленными рабочей программой учебной дисциплины;
- обобщения, систематизации, углубления, закрепления полученных теоретических знаний;
- готовности использовать теоретические знания на практике.

Практические занятия способствуют формированию в дальнейшем при изучении профессиональных модулей, следующих 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 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.

В рабочей тетради предлагаются к выполнению практические работы, предусмотренные учебной рабочей программой дисциплины «Организационно-правовое обеспечение информационной безопасности».

При разработке содержания практических работ учитывался уровень сложности освоения студентами соответствующей темы, общих и профессиональных компетенций, на формирование которых направлена дисциплина.

Рабочая тетрадь имеет практическую направленность и значимость. Формируемые в процессе практических занятий умения могут быть использованы студентами в будущей профессиональной деятельности.

Оценки за выполнение практических работ выставляются по пятибалльной системе. Оценки за практические работы являются обязательными текущими оценками по учебной дисциплине и выставляются в журнале теоретического обучения.

1. Перечень практических работ по дисциплине «Организационно-правовое обеспечение информационной безопасности»

№ раздела, темы	*Освоение умений в процессе занятия*	*Тема практического занятия*	Кол-во часов	
			практических занятий	в форме практической подготовки
Тема 1. Правовое регулирование информационной безопасности и защиты информации	использовать в профессиональной деятельности н.п.а. в области информационной безопасности и защиты информации,	Практическая работа № 1 Решение ситуационных задач с использованием н.п.а. в области информационной безопасности и защиты информации	2	2
Тема 1. Правовое регулирование информационной безопасности и защиты информации	использовать в профессиональной деятельности н.п.а. в области информационной безопасности и защиты информации, а также н.м.д. ФСБ РФ, ФСТЭК в данной области;	Практическая работа № 2 Решение ситуационных задач с использованием нормативных методических документов Федеральной службы безопасности	2	2
Тема 1. Правовое регулирование информационной безопасности и защиты информации	использовать в профессиональной деятельности н.п.а. в области информационной безопасности и защиты информации, а также н.м.д. ФСБ РФ, ФСТЭК в данной области;	Практическая работа № 3 Решение ситуационных задач с использованием методических документов Федеральной службы по техническому и экспортному контролю	2	2
Тема 2. Правовые основы защиты конфиденциальной информац	использовать в профессиональной деятельности н.п.а. в области информационной безопасности и	Практическая работа № 4 Решение ситуационных задач с использованием н.п.а. в области защиты государственной тайны	2	2

№ раздела, темы	*Освоение умений в процессе занятия*	*Тема практического занятия*	Кол-во часов	
			практических занятий	в форме практической подготовки
ии по видам тайн	защиты информации,			
Тема 2. Правовые основы защиты конфиденциальной информации по видам тайн	использовать в профессиональной деятельности н.п.а. в области информационной безопасности и защиты информации,	Практическая работа № 5 Решение ситуационных задач с использованием н.п.а. в области защиты банковской тайны	2	2
Тема 2. Правовые основы защиты конфиденциальной информации по видам тайн	разрабатывать н.м. материалы по регламентации системы организационной защиты информации;	Практическая работа № 6 Решение ситуационных задач с использованием н.п.а. в области защиты персональных данных	2	2
Тема 3. Правовые основы защиты информации в организации	разрабатывать н.м. материалы по регламентации системы организационной защиты информации;	Практическая работа № 7 Разработка проекта нормативно-методического материала по регламентации системы организационной защиты информации	2	2
Тема 4. Система правовой ответственности за утечку информации и утрату носителей информации	использовать в профессиональной деятельности н.п.а. в области информационной безопасности и защиты информации,	Практическая работа № 8 Решение ситуационных задач с использованием н.п.а. по дисциплинарной и материальной ответственности	2	2
Тема 4. Система правовой ответственности за утечку информации и утрату	использовать в профессиональной деятельности н.п.а. в области информационной безопасности и защиты	Практическая работа № 9 Анализ статей Кодекса РФ об административных правонарушениях, предусматривающих ответственность за правонарушения в сфере	2	2

№ раздела, темы	*Освоение умений в процессе занятия*	*Тема практического занятия*	Кол-во часов	
			практических занятий	в форме практической подготовки
носителей информации	информации,	информации		
Тема 4. Система правовой ответственности за утечку информации и утрату носителей информации	использовать в профессиональной деятельности н.п.а. в области информационной безопасности и защиты информации,	Практическая работа № 10 Анализ статей Уголовного кодекса РФ, предусматривающих ответственность за преступления в сфере информации	2	2
Тема 5. Правовые нормы в области защиты интеллектуальной собственности	использовать в профессиональной деятельности н.п.а. в области информационной безопасности и защиты информации,	Практическая работа № 11 Решение ситуационных задач с применением н.п.а. в области защиты авторских и патентных прав	2	2
Тема 5. Правовые нормы в области защиты интеллектуальной собственности	использовать в профессиональной деятельности н.п.а. в области информационной безопасности и защиты информации,	Практическая работа № 12 Решение ситуационных задач с применением н.п.а. в области защиты средств индивидуализации	2	2
Тема 6. Организация защиты коммерческой тайны	разрабатывать локальные акты предприятия в области организации защиты коммерческой тайны	Практическая работа № 13. Разработка перечня данных предприятия, составляющих коммерческую тайну.	2	2
		Практическая работа № 14. Разработка проекта положения о порядке обращения с конфиденциальной информацией	2	2
		Практическая работа № 15. Составление перечня	2	2

№ раздела, темы	*Освоение умений в процессе занятия*	*Тема практического занятия*	Кол-во часов	
			практических занятий	в форме практической подготовки
		должностей, имеющих доступ к коммерческой тайне.		
		Практическая работа № 16. Разработка проекта приказа о введении режима коммерческой тайны	2	2
Тема 7. Организация защиты персональных данных	разрабатывать локальные акты предприятия в области защиты персональных данных	Практическая работа № 17. Разработка положения о защите персональных данных	2	2
		Практическая работа № 18. Разработка плана мероприятий по защите персональных данных	2	2
		Практическая работа № 19. Разработка проектов документов, предусмотренных по обеспечению безопасности ПДн при их обработке в информационных системах	2	2
Тема 8. Политика безопасности предприятия	разрабатывать локальные акты предприятия в области организации защиты коммерческой тайны разрабатывать локальные акты предприятия в области защиты персональных данных	Практическая работа № 20. Разработка концепции информационной безопасности предприятия	2	2
		Практическая работа № 21 Построение технологии использования электронной подписи	2	2
Тема 9. Аудит информационной безопасности предприятия	проводить аудит состояния информационной безопасности предприятия	Практическая работа № 22. Проведение аудита состояния информационной безопасности предприятия	2	2

2. Описание порядка выполнения практических работ

Практическая работа №1
Решение ситуационных задач с использованием н.п.а. в области информационной безопасности и защиты информации

Задание 1.

Используя правовую систему КонсультантПлюс, загрузите текст Конституции РФ. Найдите три нормы, которые лежат в основе законодательства гарантирующего права человека и гражданина на информационную безопасность. При выполнении задания необходимо делать ссылку на соответствующую статью нормативного правового акта.

1.

2.

3.

Задание 2.

Расположите перечисленные нормативные правовые акты по мере убывания их юридической силы, с учетом порядка их вступления в законную силу:

1. Указ Президента РФ № 170 от 20 января 1994 года «Об основах государственной политики в сфере информатизации»
2. Конституция РФ
3. Распоряжение Администрации Санкт-Петербурга от 6 декабря 2002 года N 2532-ра «О создании Комиссии по защите информации в исполнительных органах государственной власти Санкт-Петербурга»
4. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»
5. Федеральный закон от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи»,
6. Приказ Минкомсвязи России № 582 «Об утверждении требований к функционированию систем управления сетями связи при возникновении угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования» №582 от 10 октября 2019
7. Распоряжение Комитета по информатизации и связи от 31.07.2020 № 184-р «О внесении изменений в распоряжение Комитета по информатизации и связи от 13.07.2020 № 158-р»
8. Постановление Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
9. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»;
10. Указ Президента РФ № 260 от 22 мая 2015 года «О некоторых вопросах информационной безопасности Российской Федерации»

Задание 3.

Используя правовую систему КонсультантПлюс, загрузите текст нормативного правового акта:

Федеральный закон «Об электронной подписи»

1. Проанализируйте н.п.а. по плану:

1. Название н.п.а:
2. Дата принятия:
3. Дата последнего изменения:
4. Номер н.п.а.
5. Государственный орган, принявший н.п.а:
6. Сфера регулирования:

2. Найдите в тексте закона понятия (при выполнении задания необходимо делать ссылки на соответствующую статью н.п.а.):

Ключ электронной подписи -

Корпоративная информационная система -

Электронная подпись –

3. Ответьте на вопрос (при выполнении задания необходимо делать ссылки на соответствующую статью н.п.а.):

Вправе ли Федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, устанавливать формат электронной подписи?

Практическая работа №2
Решение ситуационных задач с использованием нормативных методических документов Федеральной службы безопасности

Задание 1. Используя нормативные методические документы ФСБ России, найдите определение понятия:

Средства шифрования -

Задание 2. Используя нормативные методические документы ФСБ России, ответьте на вопрос:

Каким нормативным правовым актом ФСБ России необходимо руководствоваться при разработке средств криптографической защиты информации конфиденциального характера при обрабатывании информации конфиденциального характера в государственных органах, обладатель которой принимает меры к охране ее конфиденциальности путем установления необходимости криптографической защиты данной информации?

Задание 3.

Используя, нормативные методические документы Федеральной службы безопасности России перечислите состав и содержание организационных и технических

мер, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для 1 уровня защищенности.

Практическая работа №3
Решение ситуационных задач с использованием методических документов Федеральной службы по техническому и экспортному контролю

Задание:

Зайдите на официальный сайт Федеральной службы по техническому и экспортному контролю России - https://fstec.ru. Ознакомьтесь с её государственными функциями и услугами.

Составьте схему из нормативных правовых актов (не менее 4-х уровней н.п.а.) с соблюдением иерархии, которыми руководствуется ФСЭК России, при осуществлении функций по технической защите информации:

1) при обеспечении безопасности критической информационной инфраструктуры:
   1.
   2.
   3.
   4.
   5.
   6.
   7.
   8.
   9.
   10.

2) при лицензировании:
   1.
   2.
   3.
   4.
   5.
   6.
   7.
   8.
   9.
   10.

3) при сертификации:
   1.
   2.
   3.
   4.
   5.
   6.
   7.
   8.
   9.

10.

Практическая работа №4
Решение ситуационных задач с использованием н.п.а. в области защиты государственной тайны

Задание 1. Определите, какие степени секретности должны быть установлены в отношении следующих групп сведений (особой важности, совершенно секретные и секретные), дайте ответы со ссылками на соответствующие нормативные акты:

1) сведения в отношении контрразведывательной и оперативно-розыскной деятельности;
   Ответ:

2) сведения в области научно-технической деятельности Министерства юстиции;
   Ответ:

3) показатели, которые составляют расходную часть бюджета на текущий год;
   Ответ:

4) информация, которая составляет сведения о военных разработках завода;
   Ответ:

5) разработка ФСБ по проведении контртеррористической операции по ликвидации бандформирования;
   Ответ:

6) экономические показатели военного завода.
   Ответ:

Задание 2*. К руководителю НИИ «Магнит» Ермакову обратился начальник отдела по работе со сведениями, составляющими государственную тайну Семенов с необходимостью определения степени секретности информации, полученной в опытной лаборатории НИИ. Ермаков, ознакомившись с данной информацией и с Перечнем сведений, составляющих государственную тайну, разработанным в НИИ и не обнаружив в Перечне полученной в лаборатории информации, указал Семенову ничего не предпринимать и ждать очередной проверки соответствующими органами.
Проанализируйте эту ситуацию с точки зрения норм Закона РФ «О государственной тайне».
Ответ:

Задание 3. Выберите 1 или несколько правильных вариантов ответа, дайте ответы со ссылками на нормы соответствующих н.п.а.:

1. Какие из перечисленных сведений не могут быть отнесены к государственной тайне?
А) О фактах нарушения законности органами государственной власти и их должностными лицами
Б) О достижениях науки и техники, о научно–исследовательских работах и технологиях, имеющих важное оборонное или экономическое значение

В) О привилегиях, компенсациях и социальных гарантиях, предоставляемых государством должностным лицам, предприятиям, учреждениям и организациям
Г) Об использовании инфраструктуры Российской Федерации в целях обеспечения обороноспособности и безопасности государства
Д) О чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях

Ответ:

2. Назовите степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности
А) Конфиденциально
Б) Особой важности
В) Не подлежит разглашению
Г) Совершенно секретно
Д) Секретно

Ответ:

3. Каков срок засекречивания сведений, составляющих государственную тайну?
А) 10 лет
Б) 20 лет
В) 30 лет
Г) 50 лет
Д) Бессрочно

Ответ:
4. Какие из перечисленных обстоятельств могут являться основаниями для отказа должностному лицу или гражданину в допуске к государственной тайне?
А) Оформление его близкими родственниками документов для выезда на постоянное жительство в другие государства
Б) Религиозные убеждения
В) Уклонение его от проверочных мероприятий
Г) Национальность

Ответ:

Практическая работа №5
Решение ситуационных задач с использованием н.п.а. в области защиты банковской тайны

Задача 1. Иванова И.И. решила организовать бизнес по проведению детских праздников. Она зарегистрировалась в качестве ИП, составила несколько тематических сценариев, наняла на работу персонал. На первом собрании коллектива Иванова И.И. объявила, что все сценарии являются ее коммерческой тайной и все работники должны соблюдать требования закона, охраняющего коммерческую тайну.

1. Можно ли считать установленным режим коммерческой тайны в данном случае?
2. Какие действия должна была предпринять Иванова И.И. для того, чтобы режим коммерческой тайны был установлен?

Ответ:

1.

2.

Задача 2. Сотрудник завода разработал новое техническое устройство, которое было благополучно внедрено в работу на производстве металлообрабатывающего завода. Новое техническое устройство позволило металлообрабатывающему заводу увеличить свои доходы и занять лидирующее положение в данном производстве. Руководство завода приняло решение отнести информацию о техническом устройстве к коммерческой тайне.

Какие обязанности появляются у работодателя и работников организации в целях охраны конфиденциальности информации составляющей коммерческую тайну?

Ответ:

Задача 3. Директор ООО «777» издал приказ, согласно которому установил режим «Коммерческой тайны» к некоторой информации (список работников организации; презентация производственного оборудования; показатели производственного травматизма; перечень партнеров организации; сведения о нарушениях налогового законодательства; перечень актов административных предписаний), в связи с этим, обязал сотрудника по обслуживанию сайта удалить эту информацию с официального сайта, которая, по его мнению негативно влияла на репутацию компании.

1. Вправе ли директор компании установить режим «коммерческой тайны» в отношении перечисленной информации?

Ответ:

1. Список работников организации -
2. Презентация производственного оборудования -
3. Показатели производственного травматизма -
4. Перечень партнеров организации -
5. Сведения о нарушениях налогового законодательства -
6. Перечень актов административных предписаний -

Практическая работа №6
Решение ситуационных задач с использованием н.п.а. в области защиты персональных данных

Задание:

Используя нормативный правовой акт по защите информации содержащий требования к защите персональных данных (Постановление Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"), определите необходимый уровень защищенности ИСПДн, заполните таблицу (укажите в пустых ячейках уровень защищенности: УЗ1, УЗ2, УЗ3, УЗ4):

Уровни защищенности ИСПДн

Категории персональных данных	**Категории субъектов**	**Количество субъектов**	**Тип актуальных угроз**		
			1 тип	**2 тип**	**3 тип**
Специальные	не сотрудники оператора	более 100000			
		менее 100000			
	сотрудники оператора	любое			
Биометрические	не сотрудники оператора	более 100000			
		менее 100000			
	сотрудники оператора	любое			
Иные	не сотрудники оператора	более 100000			
		менее 100000			
	сотрудники оператора	любое			
Общедоступные	не сотрудники оператора	более 100000			
		менее 100000			
	сотрудники оператора	любое			

Практическая работа №7
Разработка проекта нормативно-методического материала по регламентации системы организационной защиты информации

Задание:
В организации разрабатывается Положение о коммерческой тайне, регламентирующее работу по защите информации. Подготовьте содержание разделов Положения, используя нормативные правовые акты:

1. «Общие положения»:

   1.2. Настоящее Положение является локальным нормативным актом и разработано в соответствии:

   (перечислите нормативные правовые акты, на основании которых разрабатывается Положение о коммерческой тайне)

6. «Режим коммерческой тайны»:

   6.1. Режим коммерческой тайны устанавливается посредством принятия следующих мер:

   (перечислите меры, посредством которых устанавливается в организации режим коммерческой тайны)

   6.2. Меры по охране конфиденциальности информации признаются разумно достаточными, если:

   (перечислите включаемые в положение условия, при которых меры по охране конфиденциальности информации признаются разумно достаточными)

Практическая работа №8
Решение ситуационных задач с использованием н.п.а. по дисциплинарной и материальной ответственности

Задание: решите ситуационные задачи.

1. Иванов, работающий в организации в должности техника по защите информации, нарушил требования должностной инструкции, за что работодатель применил выговор, а затем его уволил.

   1) *Какой вид ответственности применил работодатель?*
   2) *Проанализируйте виды наказаний относительно Трудового кодекса РФ.*

2. Техник по защите информации Петров был привлечен к материальной ответственности за причинение ущерба работодателю. В кабинете Петрова некоторое время назад стало плохо закрываться окно, о чем он сообщил своему непосредственному руководителю. Руководитель рекомендовал, плотно прикрывать окно, а носители информации

прикрывать полиэтиленом, чтобы в случае дождя вода не попала на них. Петров исполнил это поручение. После выходных Петров обнаружил, что из-за сильного ветра окно распахнулось и ветром сдуло защитную накидку, из-за сильного дождя пострадали техника и некоторые носители информации. Работодатель привлек Петрова к материальной ответственности.

Проанализируйте данную ситуацию относительно Трудового кодекса РФ.

3. Техник по защите информации Сидоров, проигнорировав требования должностной инструкции по обеспечению сохранности носителей информации, которые он использует в трудовой деятельности, взял пару носителей домой, чтобы ознакомиться с информацией находящихся на них. По дороге домой он зашел в магазин, поставил сумку в камеру хранения и после совершенной покупки, забыв про сумку пошел домой. Утром собираясь на работу, он вспомнил и сразу обратился в магазин, где получил ответ, что все ящики камеры хранения открыты и никаких оставленных вещей не было обнаружено. Через пару недель, работодатель обнаружил отсутствие носителей информации, и применил к Сидорову выговор, а также потребовал возместить ущерб, который включает: расходы по восстановлению информации и носителей, расходы на возмещение ущерба владельцу информации, а также возмещение суммы дохода компании, которые могла бы она получить, используя эти носители.

Проанализируйте ситуацию относительно Трудового кодекса РФ:

1. *Правомерность применения дисциплинарной ответственности.*
2. *Правомерность расчета суммы подлежащего возмещению ущерба.*

4. Иванову уволили за разглашение коммерческой тайны по п.п. «в» п. 6 ст. 81 Трудового кодекса РФ. Иванова обратилась в суд общей юрисдикции с требованием о восстановлении на работе. Увольнение считает незаконным по следующим основаниям. Во-первых, ее трудовой договор не содержал условие о неразглашении коммерческой тайны. Во-вторых, на материальные носители, содержащие информацию, составляющую коммерческую тайну, гриф «Коммерческая тайна» с указанием обладателя этой информации (полного наименования и места нахождения юридического лица) нанесен не был.

Подлежит ли требование Ивановой удовлетворению?

5. Бухгалтер Петрова долго спорила с начальником отдела кадров Сидоровой о способе расчета дней для компенсации работнику отпуска при увольнении на повышенных тонах, нервничая и размахивая руками. Секретарю Ивановой спор показался забавным, и она сняла разговор на камеру телефона. При этом на видео был виден бейдж Петровой с ее именем и фамилией. В этот же день видеоролик появился в общем доступе одной из социальных сетей.

Можно ли привлечь к дисциплинарной ответственности секретаря Иванову?

Практическая работа №9
Анализ статей Кодекса РФ об административных правонарушениях, предусматривающих ответственность за правонарушения в сфере информации

Задание 1: Определите состав административных правонарушений в области информации в статьях Кодекса РФ об административных правонарушениях.

Каждое правонарушение имеет свой состав, который включает 4 основных элемента, которые в задании требуется раскрыть и описать: 1) субъект (кто является правонарушителем, кто несет наказание: *ФЛ, ЮЛ, ДЛ* и др.), 2) объект (на что, какие отношения осуществляется посягательство: *общественные отношения в области информации*), 3) объективная сторона (в чем состоит противоправное деяние и каковы вредные последствия: *действие или бездействие*) и 4) субъективная сторона (какова форма вины: *умысел или неосторожность*).

Действие *- это активное, сознательное, общественно опасное, противоправное поведение субъекта.*

Бездействие *- неактивное внешнее поведение, в результате которого лицо осознанно уклоняется от того, что должно было совершить в определенной ситуации.*

Административное правонарушение признается совершенным ***умышленно****, если лицо, его совершившее, сознавало противоправный характер своего действия (бездействия), предвидело его вредные последствия и желало наступления таких последствий или сознательно их допускало либо относилось к ним безразлично.*

Административное правонарушение признается совершенным ***по неосторожности,*** *если лицо, его совершившее, предвидело возможность наступления вредных последствий своего действия (бездействия), но без достаточных к тому оснований самонадеянно рассчитывало на предотвращение таких последствий либо не предвидело возможности наступления таких последствий, хотя должно было и могло их предвидеть.*

Результаты запишите в таблицу:

Административные правонарушения в области информации

Статья	Объект	Объективная сторона	Субъект	Субъективная сторона	Мера наказания
п.1 ст. 13.11	Общественные отношения в области информации (персональных данных)	Действие	ФЛ ДЛ ЮЛ	Неосторожность	Штраф
п.2 ст. 13.11					
п.3 ст. 13.11					
п.4 ст. 13.11					

п.5 ст. 13.11					
п.1 ст. 13.12					
п.2 ст. 13.12					
п.3 ст. 13.12					
п.4 ст. 13.12					
п.5 ст. 13.12					
п.1 ст. 13.13					
п.2 ст. 13.13					
ст. 13.14					

Задание 2: Какие меры наказания применяются по вышеперечисленным статьям КоАП РФ и в чем их содержание? Ответы запишите в таблицу:

Мера наказания	Содержание наказания

Практическая работа №10
Анализ статей Уголовного кодекса РФ, предусматривающих ответственность за преступления в сфере информации

Задание 1: Ознакомьтесь со статьями Уголовного кодекса РФ: 272, 273, 274, 274.1.

Заполните таблицу:

Статья УК РФ	Количество частей в статье	Содержание преступления	Меры наказания	В чем отличие составов различных частей статьи?
272				
273				
274				
274.1				

Задание 2: Какие меры наказания применяются по вышеперечисленным статьям УК РФ и в чем их содержание? Ответы запишите в таблицу:

Мера наказания	Содержание наказания

Практическая работа №11
Решение ситуационных задач с применением н.п.а. в области защиты авторских и патентных прав

Ответьте на вопросы ситуационных задач, используя н.п.а. в области защиты авторских и патентных прав.

Задача 1. Студент 4-го курса технического ВУЗа Иванов написал в рамках курсовой работы компьютерную программу «TEST», позволяющую проводить тестирование остаточных знаний по ряду дисциплин.

Кому принадлежат личные неимущественные и исключительные права на данное программное обеспечение?

Задача 2. Сотрудник фирмы А. по собственной инициативе написал программу для ЭВМ., которую начал активно продавать, но не зарегистрировал данную программу в Федеральном агентстве по интеллектуальной собственности.

Является ли А. автором данной программы?

Кому принадлежат исключительные права на данную разработку?

Задача 3. Сотрудники Иванов и Петров предприятия ООО «ЛИК» в рамках своих трудовых обязанностей по заданию директора разработали базу данных сотрудников предприятия.

Кто является автором (правообладателем) указанной БД?

Кому принадлежат личные неимущественные и исключительные права по разработанной БД?

Практическая работа №12
Решение ситуационных задач с применением н.п.а. в области защиты средств индивидуализации

Ответьте на вопросы ситуационных задач, используя н.п.а. в области защиты авторских и патентных прав.

Задача 1.

ИП Петров, осуществляющий производство и дальнейшую продажу своей продукции, для привлечения покупателей использовал товарный знак и место происхождения продукции одной известной торговой марки. За данное правонарушение Петров уже привлекался к ответственности. При очередной продаже огромной партии продукции, покупатель обнаружил через некоторое время подделку и обратился к ИП Петрову с целью возврата товара. Петров отказался и потребовал провести экспертизу.

Каким видам ответственности подлежит Петров?

Перечислите меры наказаний, предусмотренные н.п.а. для данной ситуации.

Ответ:

Задача 2. Укажите какой вид ответственности и какие меры наказания предусмотрены законом в следующих случаях:

1) Незаконное использование наименования места происхождения товара.

Ответ:

2) Реализация товара, содержащего незаконное воспроизведение чужого товарного знака.

Ответ:

3) Незаконное использование места происхождения товара, если это деяние причинило ущерб в 500 000 руб., совершенные группой лиц по предварительному сговору.

Ответ:

4) Незаконное использование места происхождения товара, если это деяние причинило ущерб в размере 250 000 руб., совершенные неоднократно.

Ответ:

Практическая работа № 13.
«Разработка перечня данных предприятия, составляющих коммерческую тайну»

Задание:

1. Используя примерный перечень документов, отнесённых к коммерческой тайне, разработайте проект перечня данных предприятия, составляющих коммерческую тайну на предприятии
2. При разработке проекта отредактируйте текст положения с учетом особенностей Вашей организации.
3. Оформление проекта положения должно соответствовать требованиям ГОСТ 7.0.97-2016.

Текст ГОСТа можно прочитать здесь: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=303793&fld=134&dst=1000000001,0&rnd=0.8095166611318945#04404811876031962

Пример перечня конфиденциальных данных

Перечень сведений, отнесенных к конфиденциальной (служебной) информации в центральном аппарате Федерального агентства железнодорожного транспорта и подведомственных ему предприятиях, и учреждениях, утв. Приказом Федерального агентства железнодорожного транспорта от 24.01.2011 N 18

N п/п	Сведения, отнесенные к конфиденциальной (служебной) информации
I. Сведения об отраслевой	

N п/п	Сведения, отнесенные к конфиденциальной (служебной) информации
управленческой деятельности	
1	Отдельные материалы заседаний Федерального агентства железнодорожного транспорта (далее - Росжелдора) и сведения, содержащиеся в них, ограничение доступа к которым установлено решением заседания ПДТК Росжелдора
2	Сведения (информация), подготовленные Росжелдором на поступающие из органов государственной власти, предприятий, учреждений и организаций, независимо от организационно-правовой формы и формы собственности с пометкой "Для служебного пользования", "Коммерческая тайна", "Конфиденциально" и другие в части, не содержащей сведений, составляющих государственную тайну
3	Сведения, содержащие показатели государственного оборонного заказа в части, не содержащей сведений, составляющих государственную тайну
4	Сведения, содержащиеся в материалах служебной проверки (расследования), до утверждения акта (заключения) по проверке, а также если сведения, полученные в результате проверки (расследования), могут быть использованы в дальнейшем для противоправного действия (нанесения ущерба)
5	Сведения об организации работы, о конкретных мерах или проводимых мероприятиях, направленных на обеспечение информационной безопасности при осуществлении международного сотрудничества с участием представителей Росжелдора, а также содержащиеся в подготовительных или отчетных документах (формах) о проведении встречи
II. Сведения об административно-хозяйственной деятельности	
6	Сведения о персональных данных работника Росжелдора, содержащиеся в личном деле работника, кроме случаев, предусмотренных законодательством Российской Федерации
7	Сведения, получаемые при приеме гражданина на государственную гражданскую службу, необходимые для оформления допуска к государственной тайне
8	Сведения об осведомленности работника со сведениями, составляющими государственную тайну
9	Протоколы заседаний конкурсных комиссий по проведению конкурсов на замещение вакантных

N п/п	Сведения, отнесенные к конфиденциальной (служебной) информации
	должностей государственной гражданской службы
10	Акты проверок деятельности территориальных управлений и подведомственных организаций
11	Сведения о штатном расписании Росжелдора
12	Сведения о расположении структурных подразделений в здании
13	Протоколы заседаний жилищной комиссии
14	Протоколы заседаний конкурсной комиссии по проведению квалификационного экзамена и аттестации
III. Сведения о режиме секретности, мобилизационной подготовке, гражданской обороне, чрезвычайных ситуациях и транспортной безопасности	
15	Акты проверок обеспечения пропускного режима в административное здание Росжелдора
16	Сведения о результатах оценки уязвимости объектов транспортной инфраструктуры и транспортных средств, кроме тех, обеспечение безопасности которых осуществляется исключительно федеральными органами исполнительной власти
17	Сведения, содержащиеся в планах обеспечения транспортной безопасности объекта транспортной инфраструктуры и транспортного средства
18	Сведения, являющиеся информационными ресурсами единой государственной информационной системы обеспечения транспортной безопасности, подготовленные Росжелдором, за исключением выписок из реестра категорированных объектов транспортной инфраструктуры и транспортных средств
IV. Сведения о защите информации	
19	Сведения об организации обработки служебной информации на средствах вычислительной техники Росжелдора
20	Сведения, раскрывающие организацию, состояние защиты информации, или носителей информации, или информационного процесса
21	Сведения о методах, средствах или эффективности (состоянии защиты) конфиденциальной информации в автоматизированных информационных системах, средствах

N п/п	Сведения, отнесенные к конфиденциальной (служебной) информации
	вычислительной техники, других технических средствах
22	Обобщенные сведения, содержащиеся в схеме локальной вычислительной сети Росжелдора, с указанием организационно-технологических параметров или технических характеристик и мест расположения ее ответственных составных частей, информационных узлов (определены на схеме)
23	Сведения о конкретных проводимых и (или) планируемых мероприятиях по информационной безопасности конфиденциальной информации
V. Прочие сведения	
24	Сведения об организации, состоянии или расположении инженерных систем видеонаблюдения, пожарной или охранной сигнализации здания Росжелдора
25	Сведения, раскрывающие содержание планов и конкретных мероприятий по охране здания Росжелдора, помещений, в которых выполняются работы, хранятся материалы, ведутся переговоры конфиденциального характера
26	Данные охранного видеонаблюдения, фиксации системы охраны помещений, электронной системы прохода в здание

Вставьте ниже разработанный проект

Практическая работа № 2.
«Разработка проекта положения о порядке обращения с конфиденциальной информацией»

Задание:

1. Разработайте проект положения о порядке обращения с конфиденциальной информацией
2. При разработке проекта отредактируйте текст положения с учетом особенностей Вашей организации.
3. Оформление проекта положения должно соответствовать требованиям ГОСТ 7.0.97-2016.

Текст ГОСТа можно прочитать здесь: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=303793&fld=134&dst=1000000001,0&rnd=0.8095166611318945#04404811876031962

Варианты

Номер варианта	Организация
1	Отделение коммерческого банка
2	Поликлиника
3	Колледж
4	Офис страховой компании
5	Рекрутинговое агентство
6	Интернет-магазин
7	Центр оказания государственных услуг
8	Отделение полиции
9	Аудиторская компания
10	Дизайнерская фирма
11	Офис интернет-провайдера
12	Офис адвоката
13	Компания по разработке ПО для сторонних организаций
14	Агентство недвижимости
15	Туристическое агентство
16	Офис благотворительного фонда
17	Издательство
18	Консалтинговая фирма
19	Рекламное агентство
20	Отделение налоговой службы
21	Офис нотариуса
22	Бюро перевода (документов)
23	Научно проектное предприятие
24	Брачное агентство
25	Редакция газеты
26	Гостиница
27	Праздничное агентство
28	Городской архив
29	Диспетчерская служба такси
30	Комплексный центр социального обслуживания населения

Вставьте ниже разработанный проект

Практическая работа № 14.

«Составление перечня должностей, имеющих доступ к коммерческой тайне»

Задание:

1. Разработайте проект перечня должностей, которым доступна коммерческая тайна
2. При разработке проекта отредактируйте текст положения с учетом особенностей Вашей организации.
3. Оформление проекта положения должно соответствовать требованиям ГОСТ 7.0.97-2016.

Текст ГОСТа можно прочитать здесь: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=303793&fld=134&dst=1000000001,0&rnd=0.8095166611318945#04404811876031962

Варианты

Номер варианта	Организация
1	Отделение коммерческого банка
2	Поликлиника
3	Колледж
4	Офис страховой компании
5	Рекрутинговое агентство
6	Интернет-магазин
7	Центр оказания государственных услуг
8	Отделение полиции
9	Аудиторская компания
10	Дизайнерская фирма
11	Офис интернет-провайдера
12	Офис адвоката
13	Компания по разработке ПО для сторонних организаций
14	Агентство недвижимости
15	Туристическое агентство
16	Офис благотворительного фонда
17	Издательство
18	Консалтинговая фирма
19	Рекламное агентство
20	Отделение налоговой службы
21	Офис нотариуса
22	Бюро перевода (документов)
23	Научно проектное предприятие
24	Брачное агентство
25	Редакция газеты
26	Гостиница
27	Праздничное агентство
28	Городской архив
29	Диспетчерская служба такси
30	Комплексный центр социального обслуживания населения

Вставьте ниже разработанный проект

Практическая работа № 15.

«Разработка проекта приказа о введении режима коммерческой тайны»

Задание:

1. Разработайте проект приказа о введении режим коммерческой тайны
2. При разработке проекта отредактируйте текст положения с учетом особенностей Вашей организации.
3. Оформление проекта положения должно соответствовать требованиям ГОСТ 7.0.97-2016.

Текст ГОСТа можно прочитать здесь: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=303793&fld=134&dst=1000000001,0&rnd=0.8095166611318945#04404811876031962

Вставьте ниже разработанный проект

Практическая работа № 16.

«Разработка положения о защите персональных данных»

Задание:

1. Создайте или найдите в сети Интернет и адаптируйте под свою организацию проекта «Положение о защите персональных данных»
2. При разработке проекта отредактируйте текст положения с учетом особенностей Вашей организации.
3. Оформление проекта положения должно соответствовать требованиям ГОСТ 7.0.97-2016.

Текст ГОСТа можно прочитать здесь:

http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=303793&fld=134&dst=1000000001,0&rnd=0.8095166611318945#04404811876031962

Варианты

Номер варианта	Организация
1	Отделение коммерческого банка
2	Поликлиника
3	Колледж
4	Офис страховой компании
5	Рекрутинговое агентство
6	Интернет-магазин
7	Центр оказания государственных услуг
8	Отделение полиции
9	Аудиторская компания
10	Дизайнерская фирма
11	Офис интернет-провайдера
12	Офис адвоката
13	Компания по разработке ПО для сторонних организаций
14	Агентство недвижимости
15	Туристическое агентство
16	Офис благотворительного фонда
17	Издательство
18	Консалтинговая фирма
19	Рекламное агентство
20	Отделение налоговой службы
21	Офис нотариуса
22	Бюро перевода (документов)
23	Научно проектное предприятие
24	Брачное агентство
25	Редакция газеты
26	Гостиница
27	Праздничное агентство
28	Городской архив
29	Диспетчерская служба такси
30	Комплексный центр социального обслуживания населения

Вставьте ниже разработанный проект

Практическая работа № 17.

«Разработка плана мероприятий по защите персональных данных»

Задание:

1. Используя примерный план мероприятий по защите персональных данных, разработайте проект плана мероприятий по защите персональных данных на предприятии
2. При разработке проекта отредактируйте текст положения с учетом особенностей Вашей организации.
3. Оформление проекта положения должно соответствовать требованиям ГОСТ 7.0.97-2016.

Текст ГОСТа можно прочитать здесь:
http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=303793&fld=134&dst=1000000001,0&rnd=0.8095166611318945#04404811876031962

Пример плана мероприятий по защите персональных данных

1. Общие положения

Настоящий план устанавливает порядок приема, учета, сбора, поиска, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным сотрудников ОАО «_____».

Под сотрудниками подразумеваются лица, имеющие трудовые отношения с ОАО «_____».

1.1. Цель

Настоящий План является развитием комплекса мер, направленных на обеспечение защиты персональных данных, хранящихся у работодателя, посредством планомерных действий по совершенствованию организации труда.

2. Понятие и состав персональных данных

Под персональными данными сотрудников понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника, а также сведения о фактах, событиях и обстоятельствах жизни сотрудника, позволяющие идентифицировать его личность. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.

К персональным данным относятся:

- все биографические сведения сотрудника;
- образование;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- состав семьи;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- размер заработной платы;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела, личные карточки (форма Т2) и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке

сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- анкета;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии;
- и т.п.

Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом. Собственником информационных ресурсов (персональных данных) – является субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные, и который вступил (стал сотрудником) или изъявил желание вступить в трудовые отношения с работодателем. Субъект персональных данных самостоятельно решает вопрос передачи работодателю своих персональных данных.

Держателем персональных данных является работодатель, которому сотрудник добровольно передает во владение свои персональные данные. Работодатель выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

Права и обязанности работодателя в трудовых отношениях осуществляются физическим лицом, уполномоченным работодателем. Указанные права и обязанности он может делегировать нижестоящим руководителям – своим заместителям, руководителям структурных подразделений, работа которых требует знания персональных данных работников или связана с обработкой этих данных.

Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи, разглашения.

3. Принципы обработки персональных данных

Обработка персональных данных включает в себя их получение, хранение, комбинирование, передачу, а также актуализацию, блокирование, защиту, уничтожение. Получение, хранение, комбинирование, передача или любое другое использование персональных данных сотрудника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Все персональные данные сотрудника получаются у него самого. Если персональные данные сотрудника возможно получить только у третьей стороны, то сотрудник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Работодатель должен сообщить сотруднику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа сотрудника дать письменное согласие на их получение.

Не допускается получение и обработка персональных данных сотрудника о его политических, религиозных и иных убеждениях и частной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности. Пакет анкетно-биографических и характеризующих материалов (далее «Личное дело») сотрудника формируется в «Личное дело» после издания приказа о его приеме на работу. «Личное

дело» обязательно содержит личную карточку формы Т2, а также может содержать документы, содержащие персональные данные сотрудника, в порядке, отражающем процесс приема на работу: заявление сотрудника о приеме на работу; анкета; характеристика-рекомендация; результат медицинского обследования на предмет годности к осуществлению трудовых обязанностей; копия приказа о приеме на работу; расписка сотрудника об ознакомлении с документами организации, устанавливающими порядок обработки персональных данных работников, а также об его правах и обязанностях в этой области; расписка сотрудника об ознакомлении его с локальными нормативными актами организации.

Все документы хранятся в файлах, файлы содержатся в папках в алфавитном порядке фамилий сотрудников. Анкета является документом «Личного дела», представляющим собой перечень вопросов о биографических данных сотрудника, его образовании, выполняемой работе с начала трудовой деятельности, семейном положении, месте прописки или проживания и т.п. Анкета заполняется сотрудником самостоятельно при оформлении приема на работу. При заполнении анкеты сотрудник должен заполнять все ее графы, на все вопросы давать полные ответы, не допускать исправлений или зачеркивания, прочерков, помарок, в строгом соответствии с записями, которые содержатся в его личных документах. В графе "Ближайшие родственники" перечисляются все члены семьи сотрудника с указанием степени родства (отец, мать, муж, жена, сын, дочь, родные брат и сестра); далее перечисляются близкие родственники, проживающие совместно с сотрудником. Указываются фамилия, имя, отчество и дата рождения каждого члена семьи.

При заполнении анкеты и личной карточки Т2 используются следующие документы:

· паспорт;

· трудовая книжка;

· военный билет;

· документы об образовании.

«Личное дело» пополняется на протяжении всей трудовой деятельности сотрудника в данной организации. Изменения, вносимые в карточку Т2, должны быть подтверждены соответствующими документами (например, копия свидетельства о браке). Сотрудник отдела кадров, ответственный за документационное обеспечение кадровой деятельности, принимает от принимаемого на работу сотрудника документы, проверяет полноту их заполнения и правильность указываемых сведений в соответствии с предъявленными документами. При обработке персональных данных сотрудников работодатель в лице Генерального директора вправе определять способы обработки, документирования, хранения и защиты персональных данных сотрудников ОАО «_____» на базе современных информационных технологий.

Сотрудник обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен ТК РФ;
- своевременно сообщать работодателю об изменении своих персональных данных.

Сотрудник имеет право на:

- полную информацию о своих персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные сотрудника. Доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по своему выбору;

- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований. При отказе работодателя исключить или исправить персональные данные сотрудника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия.

4. Доступ к персональным данным

Персональные данные добровольно передаются сотрудником непосредственно держателю этих данных и потребителям внутри ОАО «_____» исключительно для обработки и использования в работе.

1. Внешний доступ. К числу массовых потребителей персональных данных вне ОАО «_____» можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

2. Внутренний доступ. Внутри ОАО «_____» к разряду потребителей персональных данных относятся сотрудники функциональных структурных подразделений, которым эти данные необходимы для выполнения должностных обязанностей:

- все сотрудники отдела кадров;
- все сотрудники бухгалтерии;
- руководители структурных подразделений.

В кадровом секторе хранятся личные карточки сотрудников, работающих в настоящее время. Для этого используются специально оборудованные шкафы или сейфы, которые запираются. Личные карточки располагаются в алфавитном порядке. После увольнения документы по личному составу передаются на хранение.

5. Передача персональных данных

При передаче персональных данных сотрудника работодатель должен соблюдать следующие требования:

1. Передача внешнему потребителю.

- Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

- При передаче персональных данных сотрудника потребителям (в том числе и в коммерческих целях) за пределы ОАО «_____» работодатель не должен сообщать эти данные третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника.

- Ответы на правомерные письменные запросы других фирм, учреждений и организаций даются с разрешения Генерального директора и только в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений.

- Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

- Сведения передаются в письменной форме и должны иметь гриф конфиденциальности.

- По возможности персональные данные обезличиваются.

2. Передача внутреннему потребителю.

- Работодатель вправе разрешать доступ к персональным данным сотрудников только специально уполномоченным лицам, перечисленным в п.2 гл.4.

- Потребители персональных данных должны подписать обязательство о неразглашении персональных данных сотрудников. (Приложение №1)

6. Защита персональных данных

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное

проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

1. «Внутренняя защита».

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документами и базами данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами компании. Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между сотрудниками;
- рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание сотрудниками требований нормативно – методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа сотрудниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только Генеральному директору, и в исключительных случаях, по письменному разрешению Генерального директора, руководителю структурного подразделения;
- персональные компьютеры, на которых содержатся персональные данные, должны быть защищены паролями доступа.

2. «Внешняя защита».

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного

отношения к деятельности компании, посетители, сотрудники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.

Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим компании;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

Каждый сотрудник компании, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, административную, гражданско–правовую или уголовную ответственность граждан и юридических лиц.

Отдел кадров.

Вставьте ниже разработанный проект

Практическая работа № 18.

«Разработка проектов документов, предусмотренных по обеспечению безопасности ПДн при их обработке в информационных системах»

Задание:

1. Создайте или найдите в сети Интернет и адаптируйте под свою следующие документы:

а. «Согласие на обработку персональных данных»
б. «Согласие на обработку персональных данных (в случае получения данных у третьих лиц/передачи данных третьим лицам)»
в. «Отзыв согласия на обработку персональных данных»
г. «Журнал учета согласий субъектов персональных данных»
д. «Журнал учета обращений субъектов персональных данных о выполнении их законных прав в области защиты персональных данных»
е. «Уведомление об обработке (о намерении осуществлять обработку) персональных данных», направляемое в Роскомнадзор.
ж. «Приказ о создании комиссии по проведению категорирования персональных данных и проведению инвентаризации/обследования информационных систем»
з. «Опросный лист для сбора исходных данных об ИСПДн»
и. «Акт категорирования персональных данных (перечень персональных данных»
к. «Перечень информационных систем»
л. «Акт классификации информационной системы, обрабатывающей ПДн»
м. «Приказы о допуске»
н. «Обязательство о неразглашении сведений персонального характера»

о. «Журнал учета защищаемых носителей информации»
п. «Акт на списание и уничтожение электронных носителей информации»

2. Разработать мероприятия, предусмотренные по обеспечению безопасности ПДн при их обработке в информационных системах

Варианты

Номер варианта	Организация
1	Отделение коммерческого банка
2	Поликлиника
3	Колледж
4	Офис страховой компании
5	Рекрутинговое агентство
6	Интернет-магазин
7	Центр оказания государственных услуг
8	Отделение полиции
9	Аудиторская компания
10	Дизайнерская фирма
11	Офис интернет-провайдера
12	Офис адвоката
13	Компания по разработке ПО для сторонних организаций
14	Агентство недвижимости
15	Туристическое агентство
16	Офис благотворительного фонда
17	Издательство
18	Консалтинговая фирма
19	Рекламное агентство
20	Отделение налоговой службы
21	Офис нотариуса
22	Бюро перевода (документов)
23	Научно проектное предприятие
24	Брачное агентство
25	Редакция газеты
26	Гостиница
27	Праздничное агентство
28	Городской архив
29	Диспетчерская служба такси
30	Комплексный центр социального обслуживания населения

Вставьте ниже разработанный проект

Практическая работа № 19.
«Разработка концепции информационной безопасности предприятия»

Задание:

Используя предложенные образцы, разработать концепцию информационной безопасности компании (см. вариант), содержащую следующие основные пункты (приведен **примерный** план, в который в случае необходимости могут быть внесены изменения):

1. Общие положения

Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности

1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

- Классификации угроз.
- Основные непреднамеренные искусственные угрозы.
- Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы (см. Практическую работу № 1).

3. Механизмы обеспечения информационной безопасности Предприятия

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

4. Мероприятия по реализации мер информационной безопасности Предприятия

4.1. Организационное обеспечение информационной безопасности.

- Задачи организационного обеспечения информационной безопасности.
- Подразделения, занятые в обеспечении информационной безопасности.
- Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности Предприятия.

- Общие положения.
- Защита информационных ресурсов от несанкционированного доступа.
- Средства комплексной защиты от потенциальных угроз.
- Обеспечение качества в системе безопасности.
- Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия.

- Правовое обеспечение юридических отношений с работниками Предприятия.
- Правовое обеспечение юридических отношений с партнерами Предприятия.
- Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

5. Программа создания системы информационной безопасности Предприятия

6. Варианты

Номер варианта	**Организация**

1	Отделение коммерческого банка
2	Поликлиника
3	Колледж
4	Офис страховой компании
5	Рекрутинговое агентство
6	Интернет-магазин
7	Центр оказания государственных услуг
8	Отделение полиции
9	Аудиторская компания
10	Дизайнерская фирма
11	Офис интернет-провайдера
12	Офис адвоката
13	Компания по разработке ПО для сторонних организаций
14	Агентство недвижимости
15	Туристическое агентство
16	Офис благотворительного фонда
17	Издательство
18	Консалтинговая фирма
19	Рекламное агентство
20	Отделение налоговой службы
21	Офис нотариуса
22	Бюро перевода (документов)
23	Научно проектное предприятие
24	Брачное агентство
25	Редакция газеты
26	Гостиница
27	Праздничное агентство
28	Городской архив
29	Диспетчерская служба такси
30	Комплексный центр социального обслуживания населения

Вставьте ниже разработанный проект

Практическая работа № 20.
«Построение технологии использования электронной подписи»

Задание:

- Создайте пару ключей в менеджере ключей Cleopatra.
- Экспортируйте сертификат открытого ключа из своей пары ключей в файл и передайте его своему напарнику.
- Получив файл с экспортированным ключом от напарника, импортируйте его в менеджер ключей. Установите для импортированного ключа полное доверие.
- Зашифруйте с использованием импортированного ключа напарника произвольный текст на диске. Передайте зашифрованный текст напарнику.
- Получив зашифрованный файл от напарника, дешифруйте его своим закрытым ключом. Убедитесь, что файл был успешно дешифрован.
- Используя свой закрытый ключ, подпишите произвольный файл на диске электронной подписью. Передайте подписанный документ напарнику.
- Получив от напарника документ с подписью, убедитесь, что подпись верна.

- Оформите отчет по выполненной работе.

Вставьте скриншоты выполненной работы

Практическая работа № 22.
«Проведение аудита состояния информационной безопасности предприятия»

Задание:

1. Используя план по проведению аудита, разработайте проект отчета аудита состояния информационной безопасности предприятия
2. При разработке проекта отредактируйте текст положения с учетом особенностей Вашей организации.
3. Оформление проекта положения должно соответствовать требованиям ГОСТ 7.0.97-2016.

Текст ГОСТа можно прочитать здесь:
http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=303793&fld=134&dst=1000000001,0&rnd=0.8095166611318945#04404811876031962

Пример плана по проведению аудита

1. Цель проекта
2. Подход к выполнению работ
3. Резюме для руководства о результатах проведенного аудита
4. Результаты анализа технической защищенности внешнего периметра
  4.1 Описание используемых средств
  4.2 Описание выявленных недостатков/уязвимостей в отношении внешнего периметра
5. Результаты анализа защищенности внутреннего периметра
  5.1. Область проведения
  5.2. Описание выявленных недостатков/уязвимостей в отношении внутреннего периметра
  5.3. Описание выявленных недостатков/уязвимостей в отношении DMZ
6. Рекомендуемые шаги

Вставьте ниже разработанный проект