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 МДК.05.02 Организация работы персонала с конфиденциальной информацией
ПМ.05 УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

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 для выполнения практических работ предназначена для организации работы на практических занятиях по МДК 05.02 «Организация работы персонала с конфиденциальной информацией», 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 МДК 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 по МДК 05.02 «Организация работы персонала с конфиденциальной информацией» 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.

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 поддержание 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 5.2 Проводить контроль соблюдения персоналом требований режима защиты информации

В Рабочей тетради предлагаются к выполнению практические работы, предусмотренные учебной рабочей программой МДК 05.02 «Организация работы персонала с конфиденциальной информацией».

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

Выполнение практических работ в рамках учебной дисциплины позволяет освоить комплекс работ по выполнению практических заданий по всем темам МДК 05.02 «Организация работы персонала с конфиденциальной информацией»

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

Рабочая тетрадь предназначена для студентов, изучающих МДК 05.02 «Организация работы персонала с конфиденциальной информацией».

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 ТЕМАМ МДК 05.02 ОРГАНИЗАЦИЯ РАБОТЫ ПЕРСОНАЛА С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

№ раздела, темы	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
Тема 2.1. Задачи, функции и структура подразделений защиты информации	ПК 5.2 ОК 1-11	Практическое занятие № 1 Разработка положений для подразделения защиты информации	2
		Практическое занятие № 2 Анализ положения о подразделении защиты информации организации на соответствие нормативно-правовым документам	2
Тема 2.2. Методы проверки персонала по защите информации	ПК 5.2 ОК 1-11	Практическое занятие № 3 Контролирование соблюдения персоналом требований режима защиты информации	2
Тема 2.3. Служебное расследование нарушения сотрудниками режима работы с конфиденциальной информацией	ПК 5.2 ОК 1-11	Практическое занятие № 4 Разработка положения о порядке обнаружения, анализа и реагирования на инциденты информационной безопасности организации	2
		Практическое занятие № 5 Составление отчёта об инциденте информационной безопасности и внесение инцидента в журнал учёта инцидентов ИБ	4
		Практическое занятие № 6 Анализ положения о служебных расследованиях нарушения сотрудниками режима работы с конфиденциальной информацией	2
Тема 2.5. Разрешительная система доступа к конфиденциальной информации	ПК 5.2 ОК 1-11	Практическое занятие № 7. Подготовка данных для проекта Положения о разрешительной системе доступа к конфиденциальной информации.	2
		Практическое занятие № 8. Разработка проекта Положения о разрешительной системе доступа к конфиденциальной информации.	2
		Практическое занятие № 9. Разработка проекта Положения об экспертной комиссии.	2
		Практическое занятие № 10. Разработка проекта Приказа об экспертной комиссии о защите конфиденциальной информации	2
Тема 2.6. Особенности работы с персоналом, владеющим конфиденциальной информацией	ПК 5.2 ОК 1-11	Практическое занятие № 11. Разработка номенклатуры должностей сотрудников, подлежащих оформлению на допуск к КИ.	2
		Практическое занятие № 12 Составление обязательства о неразглашении конфиденциальной информации при приеме сотрудника на работу.	2
		Практическое занятие № 13 Разработка инструкции для персонала по организации работы с конфиденциальной информацией	2
		Практическое занятие № 14. Составление	2

№ раздела, темы	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
		заявления на предоставление временного доступа.	
		Практическое занятие № 15. Разработка проекта приказа на временный доступ	2
		Практическое занятие № 16. Разработка журналов учета доступа и использования КИ	2
		Практическое занятие № 17. Подготовка памятки для персонала по организации работы с конфиденциальной информацией сотрудника при увольнении	2
		Практическое занятие № 18. Разработка проекта Инструкции по учету, обработке, хранению, передаче, использованию различных носителей конфиденциальной информации.	2
		Практическое занятие № 19. Заполнение документов по учету, обработке, хранению, передаче, использованию различных носителей конфиденциальной информации**.**	2
Тема 2.8. Организация и проведение совещаний и переговоров по конфиденциальным вопросам	ПК 5.2 ОК 1-11	Практическое занятие № 20. Решение ситуационных задач	4
Тема 2.9. Организация работы при осуществлении международного сотрудничества	ПК 5.2 ОК 1-11	Практическое занятие № 21. Разработка инструкции по защите конфиденциальной информации при работе с зарубежными партнерами.	2
Тема 2.10. Принципы, методы и технология управления подразделений по защите информации	ПК 5.2 ОК 1-11	Практическое занятие № 22 Использование критериев подбора сотрудников подразделений защиты информации	2
		Практическое занятие №23 Расстановка сотрудников подразделений защиты информации	2
		Практическое занятие №24 Составление должностных инструкций для персонала подразделений по защите информации	4
		Практическое занятие № 25 Анализ резюме на соответствие должности по профессиональному стандарту и написание своего «идеального» резюме	4

2 ОПИСАНИЕ ПОРЯДКА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа № 1 «Разработка положений для подразделения защиты информации

Цель практического занятия: научиться составлять положения для подразделений с разными видами деятельности по защите информации

Задание:

разработать положения для подразделений защиты информации, используя следующие входные данные:

Организация	
Количество сотрудников в организации	
Вид деятельности организации	

Решение:

_____

_____

(наименование должности руководителя предприятия)

_____

(Ф.И.О., подпись)

"____"_____ _____ г.

ПОЛОЖЕНИЕ

о работе подразделения _____

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Подразделение по защите информации (далее - "подразделение") является структурным подразделением службы безопасности предприятия и подчиняется непосредственно _____.

1.2. Подразделение создан на основании приказа руководителя предприятия N _____ от "__"_____ ___ г.

1.3. Начальник подразделения назначается и освобождается от должности приказом руководителя предприятия.

Работники подразделения назначаются и освобождаются от должности приказом руководителя предприятия по представлению Начальника подразделения.

1.4. Подразделение в своей работе руководствуется:

_____
_____
_____
_____
_____.

1.5. В подразделении должны быть документы и материалы:

_____
_____
_____

2. СТРУКТУРА ПОДРАЗДЕЛЕНИЯ

2.1. Структуру и штаты подразделения утверждает руководитель предприятия.

2.2. Руководство подразделения осуществляет Начальник подразделения.

2.3. В состав подразделения входят (указать должности):

_____
_____

3. ОСНОВНЫЕ ЗАДАЧИ ПОДРАЗДЕЛЕНИЯ

_____
_____
_____
_____
_____

4. ФУНКЦИИ ПОДРАЗДЕЛЕНИЯ

_____
_____
_____
_____
_____
_____
_____
_____

5. ПРАВА

Подразделение для решения возложенных на него задач имеет право:

_____
_____
_____
_____

6. ВЗАИМОДЕЙСТВИЕ СО СТРУКТУРНЫМИ ПОДРАЗДЕЛЕНИЯМИ ПРЕДПРИЯТИЯ

6.1. В процессе производственной деятельности предприятия подразделение взаимодействует со следующими структурными подразделениями:

_____
_____
_____
_____

7. ОТВЕТСТВЕННОСТЬ

7.1. Всю полноту ответственности за качество и своевременность выполнения возложенных настоящим Положением на подразделение задач и функций несет _____.

7.2. Ответственность работников подразделения устанавливается действующим законодательством и должностными инструкциями.

7.3. Начальник и другие работники подразделения несут персональную ответственность за соответствие оформляемых ими документов и операций с корреспонденцией законодательству Российской Федерации.

_____
_____
_____

_____

_____
(наименование должности руководителя
предприятия)

_____
(Ф.И.О., подпись)
"____"_____ _____ г.

ПОЛОЖЕНИЕ
о работе подразделения _____

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Подразделение по защите информации (далее - "подразделение") является структурным подразделением службы безопасности предприятия и подчиняется непосредственно _____.

1.2. Подразделение создан на основании приказа руководителя предприятия N _____ от "__"_____ ___ г.

1.3. Начальник подразделения назначается и освобождается от должности приказом руководителя предприятия.

Работники подразделения назначаются и освобождаются от должности приказом руководителя предприятия по представлению Начальника подразделения.

1.4. Подразделение в своей работе руководствуется:

_____
_____
_____

1.5. В подразделении должны быть документы и материалы:

_____
_____

2. СТРУКТУРА ПОДРАЗДЕЛЕНИЯ

2.1. Структуру и штаты подразделения утверждает руководитель предприятия.

2.2. Руководство подразделения осуществляет Начальник подразделения.

2.3. В состав подразделения входят (указать должности):

_____
_____

3. ОСНОВНЫЕ ЗАДАЧИ ПОДРАЗДЕЛЕНИЯ

_____
_____
_____
_____
_____

4. ФУНКЦИИ ПОДРАЗДЕЛЕНИЯ

_____
_____
_____
_____
_____
_____
_____

5. ПРАВА

Подразделение для решения возложенных на него задач имеет право:

_____
_____
_____
_____
_____

6. ВЗАИМОДЕЙСТВИЕ СО СТРУКТУРНЫМИ ПОДРАЗДЕЛЕНИЯМИ ПРЕДПРИЯТИЯ

6.1. В процессе производственной деятельности предприятия подразделение взаимодействует со следующими структурными подразделениями:

_____
_____
_____
_____
_____

7. ОТВЕТСТВЕННОСТЬ

7.1. Всю полноту ответственности за качество и своевременность выполнения возложенных настоящим Положением на подразделение задач и функций несет _____.

7.2. Ответственность работников подразделения устанавливается действующим законодательством и должностными инструкциями.

7.3. Начальник и другие работники подразделения несут персональную ответственность за соответствие оформляемых ими документов и операций с корреспонденцией законодательству Российской Федерации.

_____
_____
_____

_____

_____

(наименование должности руководителя предприятия)

_____

(Ф.И.О., подпись)
"____"_____ _____ г.

ПОЛОЖЕНИЕ
о работе подразделения _____

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Подразделение по защите информации (далее - "подразделение") является структурным подразделением службы безопасности предприятия и подчиняется непосредственно _____.

1.2. Подразделение создан на основании приказа руководителя предприятия N _____ от "__"_____ ___ г.

1.3. Начальник подразделения назначается и освобождается от должности приказом руководителя предприятия.

Работники подразделения назначаются и освобождаются от должности приказом руководителя предприятия по представлению Начальника подразделения.

1.4. Подразделение в своей работе руководствуется:

_____
_____

1.5. В подразделении должны быть документы и материалы:

_____
_____

2. СТРУКТУРА ПОДРАЗДЕЛЕНИЯ

2.1. Структуру и штаты подразделения утверждает руководитель предприятия.

2.2. Руководство подразделения осуществляет Начальник подразделения.

2.3. В состав подразделения входят (указать должности):

_____
_____

3. ОСНОВНЫЕ ЗАДАЧИ ПОДРАЗДЕЛЕНИЯ

_____
_____
_____
_____

4. ФУНКЦИИ ПОДРАЗДЕЛЕНИЯ

_____
_____
_____
_____
_____
_____
_____
_____
_____

5. ПРАВА

Подразделение для решения возложенных на него задач имеет право:

_____
_____
_____
_____
_____

6. ВЗАИМОДЕЙСТВИЕ СО СТРУКТУРНЫМИ ПОДРАЗДЕЛЕНИЯМИ ПРЕДПРИЯТИЯ

6.1. В процессе производственной деятельности предприятия подразделение взаимодействует со следующими структурными подразделениями:

_____
_____
_____
_____
_____

7. ОТВЕТСТВЕННОСТЬ

7.1. Всю полноту ответственности за качество и своевременность выполнения возложенных настоящим Положением на подразделение задач и функций несет _____.

7.2. Ответственность работников подразделения устанавливается действующим законодательством и должностными инструкциями.

7.3. Начальник и другие работники подразделения несут персональную ответственность за соответствие оформляемых ими документов и операций с корреспонденцией законодательству Российской Федерации.

Практическая работа № 2 «Анализ положения о подразделении защиты информации организации на соответствие нормативно-правовым документам

Цель практического занятия: научиться анализировать положения на соответствие нормативно-правовым документам

Задание:

Прочитать заданное положение об отделе защиты информации и ответить на следующие вопросы:

Какие нормативно-правовые документы не представлены в заданном положении?

_____
_____
_____

Есть ли в заданном положении информация о защите персональных данных сотрудников? Если есть, то в каком разделе? Если нет, то как и что нужно изменить в положении чтобы оно соответствовало закону о персональных данных?

_____
_____
_____

Почему в положении об отделе защиты информации должна быть информация о защите персональных данных? (ответ подтвердить статьёй из ТК РФ)

_____
_____

Какие функции выполняют сотрудники ИБ? В каком разделе эта информация представлена? Что нужно изменить в Положении, чтобы были понятны функции сотрудников? Какие функции сотрудников ИБ нужно добавить?

_____
_____
_____
_____

Что относится к должностной инструкции и нужно убрать из Положения?

_____
_____

Как и с кем взаимодействуют сотрудники отдела ИБ? Что нужно добавить в Положение?

_____
_____
_____
_____

Какую информацию защищают сотрудники ИБ? Понятно ли это из Положения?

_____
_____

Сколько подразделений защиты информации в данной организации?

_____

Сколько сотрудников входит в отдел защиты информации по данному Положению?

_____

Приложение к практической работе № 2

УТВЕРЖДАЮ
Генеральный директор
Ю.З. Ернеймов

ПОЛОЖЕНИЕ _____ №_____
Об отделе защиты информации

I.ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Отдел защиты информации осуществляет организацию и координацию работ подразделений организацию ОАО «Биннофарм» по комплексной защите информации, контроль и оценку эффективности принятых мер по обеспечению информационной безопасности ОАО «Биннофарм».

1.2.Отдел защиты информации возглавляется начальником отдела. Начальник отдела назначается на должность и освобождается от занимаемой должности в установленном порядке по представлению руководителя организации ОАО «Биннофарм».

1.3.Структура и штатное расписание отдела определяются в установленном порядке, в соответствии с объемами работ, задачами и функциями, исполняемыми отделом.

1.5.В своей деятельности отдел руководствуется действующим законодательством, Уставом ОАО «Биннофарм».

II. ЦЕЛИ И ЗАДАЧИ

2.1.Основной целью отдела ИБ является:

2.1.1. Организация защиты информации на ОАО «Биннофарм».

2.2. Основными задачами отдела ИБ являются:

2.2.1. Оснащение помещения программно-аппаратными средствами ОАО «Биннофарм».

2.2.2. Подготовка кадров для работы с КИ.

2.2.3. Организация правовой ЗИ.

III. СТРУКТУРА

3.1. Структура и должностной состава отдела ЗИ утверждается руководством ОАО «Биннофарм» с учетом специфики объема работы.

3.2. В состав отдела ИБ входят следующие должности:

- Специалист по защите информации.
- Главный специалист по защите информации.
- Оператор видеонаблюдения.
- Специалист по подготовке кадров.

IV. РУКОВОДСТВО

4.1. Отдел ИБ возглавляет руководитель отдела ИБ, который назначается и освобождается руководителем ОАО «Биннофарм».

4.2. Должностные обязанности, права и ответственность определены в должностной инструкции руководителя отдела ИБ.

4.3. Руководитель отдела ИБ:

4.3.1. Организует разработку и внедрение организационных и технических мероприятий по комплексной защите информации на предприятии, ведущем работы, содержание которых составляет государственную или коммерческую тайну, обеспечивает соблюдение режима проводимых работ и сохранение конфиденциальности документированной информации.

4.3.2. Руководит проведением работ по организации, координации, методическому руководству и контролю их выполнения по вопросам защиты информации и разработкой технических средств контроля, определяет перспективы их развития.

4.3.3. Обеспечивает взаимодействие и необходимую кооперацию соисполнителей работ по вопросам организации и проведения научно-исследовательских и опытно-конструкторских разработок, организует и контролирует выполнение плановых заданий, договорных обязательств, а также сроки, полноту и качество работ, выполняемых соисполнителями.

4.3.4. Организует работу по заключению договоров на работы по защите информации, принимает меры по обеспечению финансирования работ, в том числе выполняемых по договорам.

4.3.5. Организует проведение специальных исследований и контрольных проверок по выявлению демаскирующих признаков и возможных каналов утечки информации, в том числе по техническим каналам, разрабатывает меры по их устранению и предотвра-

щению, а также работу по составлению актов и другой технической документации о степени защищенности технических средств и помещений.

4.3.6. Организует рассмотрение применяемых и предлагаемых методов защиты информации, промежуточных и конечных результатов исследований и разработок.

4.3.7. Обеспечивает соблюдение режима проводимых работ и сохранение конфиденциальности документированной информации.

4.3.8. Возглавляет разработку проектов перспективных и текущих планов работы.

4.3.9. Ведет переговоры с ведущими специалистами в области ЗИ по вопросам ИБ.

V. ДЕЯТЕЛЬНОСТЬ

5.1. Деятельность сотрудников отдела ИБ осуществляется на основании нормативно-правовых документов в ОАО «Биннофарм» и должностных инструкций.

5.2. В соответствии с целями и задачами отдела, сотрудники отдел осуществляют:

5.2.1. Установку межсетевых экранов.

5.2.2. Организацию охраны помещений.

5.2.3.Осуществляют настройку технических средств защиты.

5.2.4. Поводят обучение сотрудников.

5.2.5. Проводят аттестацию персонала.

5.2.6. Регламентируют состав информации ограниченного доступа.

5.2.7. Разрабатывают правила работы с информацией ограниченного доступа и обучение сотрудников этим правилам.

VI. ПРАВА И ОТВЕТСТВЕННОСТЬ

6.1. Сотрудники отдела ИБ имеют право:

6.1.1. Использовать информацию открытого и ограниченного доступа.

6.1.2. Привлекать в установленном порядке руководство и специалистов структурных подразделений к подготовке проектов организационно-правовых документов ОАО «Биннофарм».

6.2. Сотрудники отдела ИБ несут ответственность за:

6.2.1. В соответствии с законодательством сотрудники отдела ИБ несут дисциплинарную, административную либо гражданско-правовую ответственность за:

6.2.1.1. Разглашение информации, содержащую конфиденциальные данные ОАО «Биннофарм».

6.2.1.2. Уничтожение конфиденциальной информации умышленно или неосторожно.

6.2.2. Неисполнение требований организационно-правовых документов ОАО «Биннофарм».

6.2.3. Неисполнение должностных обязанностей согласно данному положению, должностным инструкциям и трудовым договорам.

VII. ВЗАИМОДЕЙСТВИЕ СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ С ДРУГИМИ СТРУКТУРНЫМИ ПОДРАЗДЕЛЕНИЯМИ

7.1. Взаимодействие отдела со сторонними российскими организациями по вопросам защиты информации осуществляется на основании законодательства РФ и договорных документов, заключенных с ними.

7.2. Со всеми подразделениями предприятия по вопросам: заявок на сопровождение работников предприятия, перевозящих товарно-материальных ценности; - данных о мерах, принятых к обеспечению сохранности товарно-материальных ценностей предприятия; - сведений об угрозах в адрес руководящих работников предприятия; - информации об утрате, гибели имущества предприятия;

- рекомендаций и разъяснений по соблюдению режима охраны на предприятии; - групп сопровождения для перевозки товарно-материальных ценностей;

VIII. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Деятельность отдела ведется согласно Инструкции по обеспечению защиты информации ОАО «Биннофарм».

8.2. Решение об изменении, дополнении и аннулировании данного Положения принимает руководство ОАО «Биннофарм» в установленном порядке.

8.3. Процесс реорганизации и ликвидации отдела определен в Положении о структурных подразделениях ОАО «Биннофарм».

Руководитель отдела ИБ В.А.Соктов

СОГЛАСОВАНО

Юрисконсульт

А.И. Тронов

В дело № _____

Практическая работа № 3 «Контролирование соблюдения персоналом требований режима защиты информации»

Цель практического занятия: научиться составлять план контроля за сотрудниками по соблюдению требований защиты информации

Задание:

Составить инструкцию для специалиста по защите информации по контролированию соблюдения персоналом требований режима защиты информации

Инструкция для специалиста по защите информации по контролированию соблюдения персоналом требований режима защиты информации

1. Общие положения

1.1. Настоящая Инструкция относится к _____

_____

1.2. В настоящей Инструкции определен _____

_____.

1.3. Настоящая Инструкция разработана с целью _____

_____.

2. Подразделения, подлежащие контролю

2.1. _____

2.1.1. Требования режима защиты информации:_____

_____

2.2. _____

2.2.1. Требования режима защиты информации:_____

_____

2.3. _____

2.3.1. Требования режима защиты информации:_____

_____

2.4. _____

2.4.1. Требования режима защиты информации:_____

_____

2.5. _____

2.5.1. Требования режима защиты информации:_____

_____

2.6. _____

2.6.1. Требования режима защиты информации:_____

_____

3. Методы контроля соблюдения персоналом требований режима защиты информации

3.1. _____

3.2. _____

3.3. _____

3.4. _____

3.5. _____

3.6. _____

4. Сроки проведения контроля соблюдения персоналом требований режима защиты информации

4.1. _____

4.2. _____

4.3. _____

4.4. _____

4.5. _____

4.6. _____

5. Ответственность за контролирование соблюдения персоналом требований режима защиты информации

_____

_____

Практическая работа № 4 «Разработка положения о порядке обнаружения, анализа и реагирования на инциденты информационной безопасности организации»

Цель практического занятия: научиться писать положения о порядке обнаружения и реагирования на инциденты информационной безопасности

Задание:

Составить положение о порядке обнаружения, анализа и реагирования на инциденты информационной безопасности организации

Положение о порядке обнаружения, анализа и реагирования на инциденты информационной безопасности организации

1. Общие положения

1.1. Настоящее Положение определяет _____
_____.

1.2. Настоящее Положение разработано на основании следующих нормативно-правовых актов РФ

_____
_____.

2. Термины и определения

В настоящем Положении используются следующие термины и определения:

2.1. Инцидент ИБ _____
_____

2.2. Обработка инцидентов ИБ _____
_____

2.3. Закрытие инцидента ИБ _____
_____

3. Цели и задачи обработки Инцидентов ИБ

3.1. Основными целями обработки Инцидентов ИБ являются:

_____
_____
_____
_____

3.2. Основными задачами обработки Инцидентов ИБ являются:

_____
_____
_____
_____

4. Обнаружение Инцидентов ИБ

4.1. Обнаружение Инцидентов ИБ выполняется _____
_____

4.2. Регистрация информации об Инцидентах ИБ, включая сбор информации, связанной с Инцидентом ИБ, выполняется _____
_____

4.3. Основными источниками информации об Инцидентах ИБ, связанных с нарушениями требований к обеспечению защиты информации _____

_____

5. Порядок анализа и реагирования на Инциденты ИБ

5.1. Анализ Инцидентов ИБ выполняется на основе: _____

_____

_____

5.2. В процессе анализа устанавливаются причины возникновения выявленных Инцидентов ИБ.

5.3. В процессе анализа определяются наиболее проблемные с точки зрения подверженности Инцидентам ИБ сегменты и компоненты информационной инфраструктуры

5.4. В процессе анализа Инцидентов ИБ оценивается достаточность принятых мер и выделенных ресурсов для реагирования на Инциденты ИБ, проводится оценка результатов реагирования на выявленные Инциденты ИБ.

5.5. В процессе анализа проверяются действия _____

Целью проведения данной проверки является формирование (инициирование) совершенствований в части

_____

_____

5.6. По результатам анализа Инцидентов ИБ формируют отчёты по результатам обработки Инцидентов ИБ.

Практическая работа № 5 «Составление отчёта об инциденте информационной безопасности и внесение инцидента в журнал учёта инцидентов ИБ»

Цель практического занятия: научиться работать с отчётом об инцидентах ИБ, написанию отчёта

Задание:

Составить отчёт об двух инцидентах информационной безопасности и внести эти инциденты в журнал учёта инцидентов ИБ:
— первый инцидент основан на человеческом факторе;
— второй инцидент основан на программном обеспечении

ОТЧЁТ об инциденте информационной безопасности № __
(номер вносится в журнал)

Инцидент зафиксирован _____
(дата, фамилия и инициалы работника (-ов))

В инциденте задействованы следующие работники

_____
(фамилия и инициалы работника (-ов))

Описание инцидента

_____

_____

_____

Причины инцидента

_____

_____

Меры, принятые для устранения причин, последствий инцидента

_____

_____

_____

_____ _____

(Должность сотрудника ИБ) Фамилия И.О.

«___» _____ 201__ г.

ОТЧЁТ об инциденте информационной безопасности № __

(номер вносится в журнал)

Инцидент зафиксирован _____

(дата, фамилия и инициалы работника (-ов))

В инциденте задействованы следующие работники

_____

(фамилия и инициалы работника (-ов))

Описание инцидента

_____

_____

_____

Причины инцидента

_____

_____

Меры, принятые для устранения причин, последствий инцидента

_____

_____

_____

_____ _____

(Должность сотрудника ИБ) Фамилия И.О.

«___» _____ 201__ г.

ЖУРНАЛ учета инцидентов информационной безопасности

Начат «___»_____

20__

Окончен «___»_____

20__

Ответственный за ведение журнала:

Должность	Фамилия И.О.	Дата назначения ответственным	Подпись

№ п/п	№ отчета об инциденте	Дата совершения инцидента	Краткое описание инцидента (заражение вирусом, компьютерная атака, утечка информации, сбой в работе оборудования и проч.)	Сроки устранения инцидента	Подпись лица, зарегистрировавшего инцидент в журнале
			_____ _____		
			_____ _____ _____		

Практическая работа № 6«Анализ положения о служебных расследованиях нарушения сотрудниками режима работы с конфиденциальной информацией»

Цель практического занятия: научиться анализировать положения о служебных расследованиях, понимать чего не хватает в положениях и исправлять их

Задание:

1. Прочитать отрывок Положения о служебных расследованиях нарушения сотрудниками режима работы с конфиденциальной информацией (В Приложении)
2. С помощью вопросов провести анализ данного положения на полноту информативности данного положения и на соответствие современным возможностям инцидентов ИБ

Срок проведения служебного расследования в Положении: _____

Ваше мнение о сроке проведения служебного расследования: _____

_____

Режим каких тайн должен быть введён в организации, чтобы проводить служебное расследование по данному Положению:

_____

_____

Какие варианты утечки информации рассмотрены в Положении: __ _____

_____

Какие варианты утечки информации НЕ рассмотрены в Положении: _____

_____

_____

Права, которые нужно добавить для членов комиссии по проведению служебного расследования: _____

_____

Каким образом можно рассчитать ущерб от утечки конфиденциальной информации:

_____

_____

_____

Цель служебного расследования: _____

_____

_____

Кто назначает комиссию для служебного расследования: _____

_____.

Приложение к практической работе 10

Проведение служебного расследования по фактам утечки конфиденциальной информации

Для проведения служебного расследования руководитель предприятия не позднее следующего дня (после обнаружения факта разглашения конфиденциальной информации или утраты носителей, содержащих такую информацию), назначает комиссию из компетентных и не заинтересованных в исходе дела сотрудников предприятия.

В состав комиссии входят не менее трех человек (включая работника режимно-секретного подразделения), имеющих непосредственное отношение к данным сведениям и допуск к государственной тайне по соответствующей форме (соответствующий допуск к конфиденциальной информации). При необходимости указанные работники освобождаются от исполнения своих служебных обязанностей на время проведения служебного расследования. В работе комиссии могут принимать участие представители вышестоящей организации (если она имеется).

Факт выявления нарушения режима коммерческой (служебной) тайны должен быть зафиксирован документально — в виде служебной записки, заявления, рапорта, акта и т. п. На основании этого документа назначается внутреннее расследование. Если факт нарушения не зафиксирован, но есть предположение о его совершении (или сокрытии факта нарушения) назначается соответствующая внутренняя проверка. Результаты проверки также могут стать основанием для проведения расследования.

Служебное расследование должно проводиться в предельно короткий срок (не более месяца со дня обнаружения факта разглашения конфиденциальной информации или утраты ее носителей).

Если утраченные носители информации не обнаружены, исчерпаны все возможные меры розыска, внесена ясность в обстоятельства произошедшего и установлены виновные, розыск может быть прекращен. Мотивированное заключение о прекращении розыска утверждается руководителем предприятия, назначившим комиссию по проведению слу-

жебного расследования, после чего оно рассматривается и утверждается руководителем вышестоящей организации (если она имеется).

Обязанности членов комиссии по проведению служебного расследования

- установить обстоятельства разглашения конфиденциальной информации или утраты содержащих ее носителей (время, место, способ и др.);
- вести розыск утраченных носителей информации;
- установить лиц, виновных в разглашении конфиденциальной информации или утрате ее носителей;
- установить причины и условия, способствующие разглашению конфиденциальной информации, утрате носителей информации, и выработать рекомендации по их устранению.

Права членов комиссии по проведению служебного расследования

Члены комиссии по проведению служебного расследования имеют право:

- проводить осмотр помещений, участков местности, хранилищ, столов, шкафов, папок, портфелей и других предметов, где могут находиться утраченные носители конфиденциальной информации;
- проверять полистно все носители конфиденциальной информации, находящиеся на предприятии, и учетные документы, отражающие их поступление и движение (книги и журналы учета);
- опрашивать работников, предприятия, допустивших разглашение конфиденциальной информации или утрату носителей этой информации, а также других работников, могущих оказать содействие в установлении обстоятельств разглашения информации (утраты носителей информации), и получать от них письменные объяснения;
- привлекать с разрешения руководства предприятия других работников предприятия, не заинтересованных в исходе дела, для проведения отдельных действий в рамках служебного расследования.

Работник, в отношении которого проводится расследование, должен быть ознакомлен с приказом (распоряжением) о проведении расследования.

Требование от работника объяснения в письменной форме для установления причины нарушения является обязательным. В случае, когда работник отказывается дать письменные объяснения, его устные показания или отказ от них письменно фиксируются членами комиссии (не менее чем за двумя подписями).

В целях исключения возможности какого-либо воздействия на процесс расследования члены комиссии обязаны соблюдать конфиденциальность расследования до принятия по ним решения руководителем организации (предприятия).

Для организованного и оперативного проведения внутреннего расследования комиссия разрабатывает версии причин нарушения (например, о возможном местонахождении пропавшего документа) и составляет план про ведения необходимых мероприятий (поиска) по каждой из этих версий. В ходе расследования могут выдвигаться и отрабатываться дополнительные версии (с соответствующим уточнением плана действий).

После того как возможные меры поиска документа (носителя, изделия) исчерпаны, но не привели к его обнаружению, полностью выяснены обстоятельства утраты и установлены виновные лица, поиск документа может быть прекращен. Решение о прекращении поиска утверждается должностным лицом, назначившим внутреннее расследование (по мотивированному заключению комиссии).

Одновременно с комиссией по проведению внутреннего расследования руководитель организации (предприятия) может поручить экспертной комиссии организации

(предприятия) определить актуальность утраченной (разглашенной) конфиденциальной информации, а также назначить комиссию по определению (подсчету) ущерба (убытков) по расследуемому факту, из компетентных и незаинтересованных должностных лиц. Указанные задачи могут возлагаться на одну комиссию (с назначением в ее состав соответствующих специалистов).

Сумма ущерба либо убытков и методика ее расчета должны быть обоснованы и утверждены. В отдельных случаях такая оценка может быть осуществлена специализированной организацией.

Цели служебного расследования

- поиск утраченного документа (носителя, изделия); изучение (анализ) ситуации для принятия мер по предотвращению (пресечению) повторения выявленного нарушения;
- создание доказательной базы для привлечения виновных лиц к установленной законодательством ответственности.

Задачи служебного расследования

- установление обстоятельств нарушения, в том числе времени, места и способа его совершения;
- обследование мест возможного нахождения утраченного конфиденциального документа (носителя, изделия и т. п.);
- установление лиц, непосредственно виновных в данном нарушении;
- выявление причин и условий, способствовавших нарушению.

Практическая работа № 7
«Подготовка данных для проекта Положения о разрешительной системе доступа к конфиденциальной информации»

Задание:

1. В верхнем колонтитуле укажите свою фамилию и инициалы.
2. Используя информационные ресурсы сети интернет, заполните исходные данные об организации.

При поиске информации руководствуйтесь следующими требованиями:

- область деятельности компании – производство и разработка ПО, консалтинг в области защиты информации или информационных технологий, продажа готового ПО, интернет технологии;
- штатная численность сотрудников не должна превышать 50 человек.

1. Полное название организации с указанием организационно-правовой формы

2. Вид деятельности

3. Перечень услуг

4. Реквизиты организации

Юридический адрес	
Фактический адрес	
Телефон факс	
e-mail	
ИНН	
КПП	
ОГРН	
ОКПО	

4. Организационная структура

5. Перечень программного обеспечения

Общесистемное ПО

№	Название	Назначение
1.		
2.		

Специализированное ПО

№	Название	Назначение
1.		
2.		

6. Перечень аппаратного обеспечения

7. Наличие корпоративной сети

8. Каналы связи, используемые для передачи информации

Практическая работа № 8
«Разработка проекта Положения о разрешительной системе доступа к конфиденциальной информации»

Задание:

1. В верхнем колонтитуле укажите свою фамилию и инициалы.
2. Разработайте и оформите проект Положения о разрешительной системе доступа к конфиденциальной информации.

Проект Положения должен содержать следующие разделы:

1. Общие положения
2. Круг лиц, имеющих право давать разрешение на доступ к конфиденциальной информации.
3. Порядок оформления разрешений на доступ к конфиденциальной информации.

Вставьте текст положения

Практическая работа № 9
«Разработка Положения об экспертной комиссии»

Задание:

1. В верхнем колонтитуле укажите свою фамилию и инициалы.
2. Разработайте и оформите проект Положения об экспертной комиссии по защите конфиденциальной информации.

Проект Положения должен содержать следующие разделы:

1. Общие положения.

   Раздел должен содержать следующую информацию:

   1.1. Что представляет собой экспертная комиссия по доступу к конфиденциальной информации.

   1.2. Перечень нормативно-правовых документов, которыми экспертная комиссия руководствуется в свое деятельности.

2. Основные цели и задачи экспертной комиссии по защите конфиденциальной информации.

   Раздел должен содержать перечень целей и задач, которые решает экспертная комиссия по защите конфиденциальной информации (не путать с функциями!)

3. Состав экспертной комиссии по защите конфиденциальной информации.

В разделе необходимо указать должностной состав экспертной комиссии по защите конфиденциальной информации применительно к Вашей организации, а также описать порядок определения персонального состава экспертной комиссии по защите конфиденциальной информации.

4. Функции экспертной комиссии по защите конфиденциальной информации.

В разделе перечисляются функции экспертной комиссии по защите конфиденциальной информации. Перечисляются только те функции, которые актуальны для Вашей организации.

5. Организация работы экспертной комиссии по защите конфиденциальной информации.

В разделе пишем следующее:
5.1. Экспертная комиссия по защите конфиденциальной информации работает по плану, утвержденному руководителем ООО «….».
5.2. Заседания экспертной комиссии и принятые на нем решения считаются правомочными, если в голосовании приняли участие не менее половины членов экспертной комиссии. Право решающего голоса имеют только члены экспертной комиссии. Приглашенные консультанты и эксперты имеют право совещательного голоса, в голосовании не участвуют. Решение принимают простым большинством голосов, при разделении голосов поровну решение принимает председатель экспертной комиссии.
5.3. Все совещания экспертной комиссии по защите конфиденциальной информации и принятые в ходе совещаний решения фиксируются в протоколе совещания.

Практическая работа № 10
«Разработка проекта приказа об экспертной комиссии по защите конфиденциальной информации»

Задание

1. В верхнем колонтитуле укажите свою фамилию и инициалы.
2. Разработайте и оформите проект Приказа об экспертной комиссии по защите конфиденциальной информации с учетом данных Вашей организации.

Приказ должен быть оформлен в соответствии с требованиями по оформлению организационно-распорядительных документов.

Вставьте скриншот приказа.

Практическая работа № 11
«Разработка номенклатуры должностей сотрудников, подлежащих оформлению на допуск к КИ»

Задание

1. В верхнем колонтитуле укажите свою фамилию и инициалы.

2. Разработайте и оформите номенклатуры должностей сотрудников, подлежащих оформлению на допуск к КИ **с учетом данных Вашей организации**.

При заполнении таблицы используйте следующие степени конфиденциальности: конфиденциально, строго конфиденциально.

Номенклатура должностей сотрудников,
подлежащих оформлению на допуск к конфиденциальной информации

Подразделение	Количество работающих	Должность	Обоснование необходимости допуска	Количество лиц, подлежащих оформлению на доступ к КИ				Количество лиц, оформленных на доступ к КИ
				Вид КИ	Степень конфиденциальности 1	Степень конфиденциальности 2	Степень конфиденциальности …	

В номенклатуре должны обязательно присутствовать грифы утверждения, согласования и подпись.

Вставьте проект номенклатуры.

Практическая работа № 12
«Составление обязательства о неразглашении
конфиденциальной информации при приеме сотрудника на работу»

Задание

1. В верхнем колонтитуле укажите свою фамилию и инициалы.

2. Составьте обязательство (соглашение) о неразглашении конфиденциальной информации при приеме сотрудника на работу **с учетом данных Вашей организации**.

При заполнении документа необходимо указать следующие реквизиты:

РАБОТОДАТЕЛЬ:

Наименование: _____

_____

Адрес: _____
(юридический и фактический)

ИНН, КПП_____

_____

_____

(должность, Ф.И.О. должностного лица)

Телефон _____

_____

М.П. (дата, подпись)

РАБОТНИК:

Ф.И.О _____

_____

Дата рождения _____

Серия и номер паспорта _____

_____

Адрес: _____
(по месту регистрации и проживания)

ИНН_____

СНИЛС_____

Телефон _____

_____

(дата, подпись) (Ф.И.О. полностью)

Шаблон (**шаблон не изменять!**):

Соглашение о конфиденциальности и неразглашении информации

г. _____ «___» _____ 202_ г.

«Организация», именуемое в дальнейшем «Работодатель», в лице руководителя _____, действующего на основании _____, с одной стороны, и _____, именуемый в дальнейшем "Работник", с другой стороны, заключили настоящее соглашение о неразглашении конфиденциальной информации, далее – «Соглашение», о нижеследующем:

1. Предмет соглашения

1.1. Работник принимает на себя обязательство не разглашать сведения, составляющие конфиденциальную информацию Работодателя, ставшие известными ему в связи с работой в Организации.

1.2. Под конфиденциальной информацией в Соглашении понимается любая информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и к сохранению конфиденциальности которой обладатель принимает все возможные меры.

1.3. Перечень информации, относящейся к конфиденциальной информации, определен в Перечне конфиденциальной информации Организации.

2. Права и обязанности сторон

2.1. Работник обязуется не разглашать сведения, составляющие конфиденциальную информацию Работодателя, ставшие ему известными в связи с работой в Организации, а также защищать вышеуказанные сведения от посягательств и попыток их обнародовать третьими лицами.

2.2. Работник обязуется использовать сведения, полученные при исполнении своих трудовых обязанностей, лишь в интересах Работодателя.

2.3. Работник обязуется после окончания работы в Организации не использовать информацию, полученную в связи с работой в Организации, в целях конкуренции с другими компаниями.

2.4. Вся информация, составляющая конфиденциальную информацию и полученная Работником в материальной (схемы, рисунки, письма, фотографии и пр.) и нематериальной формах, является собственностью Работодателя и используется только на условиях Соглашения.

2.5. При прекращении трудового договора Работник обязуется вернуть все сведения, полученные от другой стороны на материальных носителях, а также их копии, в течение одного дня с момента первого требования.

2.6. В случае разглашения сведений, составляющих конфиденциальную информацию по настоящему соглашению, Работник обязан в полном объеме возместить понесенные Работодателем в результате такого разглашения убытки, размер которых определяется независимой экспертной комиссией.

2.7. Работник подтверждает, что предупрежден о том, что в соответствии с законодательством РФ разглашение сведений, составляющих конфиденциальную информацию, может повлечь гражданско-правовую, административную и уголовную ответственность.

4. Срок действия соглашения

3.1. Настоящее соглашение вступает в силу с момента его подписания и действует в течение трех лет с момента прекращения трудового договора.

5. Непреодолимая сила (форс-мажорные обстоятельства)

4.1. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по настоящему соглашению, если неисполнение явилось следствием природных явлений, действий внешних объективных факторов и прочих обстоятельств непреодолимой силы, за которые стороны не отвечают и предотвратить неблагоприятное воздействие которых они не имеют возможности.

6. Заключительные положения

5.1. Соглашение заключено в 2-х экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой Стороны.

5.2. Любая договоренность между Сторонами, влекущая за собой новые обязательства, которые не вытекают из Соглашения, должна быть подтверждена Сторонами в форме дополнительных соглашений к нему. Все изменения и дополнения к Соглашению считаются действительными, если они оформлены в письменном виде и подписаны надлежащими уполномоченными представителями Сторон.

5.3. Сторона не вправе передавать свои права и обязательства по Соглашению третьим лицам без предварительного письменного согласия другой Стороны.

5.4. Стороны соглашаются, что за исключением сведений, которые в соответствии с законодательством Российской Федерации не могут составлять конфиденциальную информацию юридического лица, содержание Соглашения, а также все документы, переданные Сторонами друг другу в связи с его заключением, считаются конфиденциальными и относятся к тайне Сторон, которая не подлежит разглашению без письменного согласия другой Стороны.

5.5. Стороны договорились, что споры и разногласия, которые могут возникнуть между Сторонами и вытекающие из настоящего соглашения или в связи с ним, будут разрешаться путем переговоров. В случае невозможности путем переговоров достичь соглашения по спорным вопросам в течение 15 (пятнадцати) календарных дней с момента получения письменной претензии, споры разрешаются в суде г. _____ по месту регистрации Организации.

7. Адреса и реквизиты Сторон

Вставьте ниже заполненный документ

Практическая работа № 13
«Разработка инструкции для персонала по организации работы с конфиденциальной информацией»

Задание

1. В верхнем колонтитуле укажите свою фамилию и инициалы.

2. Составьте и оформите инструкцию для персонала по организации работы с конфиденциальной информацией **с учетом данных Вашей организации**.

При оформлении инструкции необходимо выполнить следующие требования:

1. Инструкция оформляется на бланке организации.
2. Инструкция должна быть утверждена руководителем организации
3. Инструкция должна быть согласована экспертной комиссией по защите конфиденциальной информацией.
4. Инструкция должна быть подписана составителем, которым является руководитель службы безопасности.
5. Инструкция должна обязательно содержать гриф ознакомления сотрудника с инструкцией.

Правила оформления грифов и реквизитов приведены в 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

Шаблон (**шаблон не изменять!**):

ИНСТРУКЦИЯ ПО РАБОТЕ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

ООО «…»

1. Общие положения

1.1. Настоящая инструкция разработана в соответствии с требованиями законодательства Российской Федерации и учредительными документами ООО «…» (далее - Организация). Она предусматривает организационные и административные меры по защите конфиденциальной информации с целью предотвращения нанесения возможного экономического и морального ущерба Организации со стороны юридических и физических лиц, вызванного их неправомерными или неосторожными действиями путем присвоения или разглашения конфиденциальной информации.

1.2. Под конфиденциальной информацией понимается сведения, связанные с задачами, решаемыми Организацией в соответствии с учредительными документами, информация, связанная с управлением, финансами и другими сферами деятельности Организации, разглашение (искажение, передача, утечка и т.д.) которой может нанести ущерб интересам Организации. К сведениям, составляющим конфиденциальную информацию, относятся сведения, предусмотренные «Перечнем сведений, составляющих конфиденциальную информацию», утвержденным и введенным в действие приказом руководителя Организации № … от ….

1.3. Разглашением конфиденциальной информации следует считать следующие действия сотрудника:

- доведение до сведения неуполномоченных лиц в устной, письменной, электронной или иной форме конфиденциальную информацию. Указанный факт может наступить

в результате умысла сотрудника или по неосторожности, включая халатное отношение к своим обязанностям;

- использование конфиденциальной информации в процессе выполнения работы для другого предприятия, учреждения и организации или по заданию физического лица, иного субъекта предпринимательской деятельности без образования юридического лица;
- использование конфиденциальной информации в научной и педагогической деятельности;
- использование конфиденциальной информации в личных целях, не связанных с выполнением должностных обязанностей в Организации;
- использование конфиденциальной информации в ходе публичных выступлений, интервью и т.п.;
- иные действия сотрудника, в результате которых конфиденциальная информация, стала известна неуполномоченным лицам.

1.4. Не считаются разглашением конфиденциальной информации действия сотрудника, указанные в п.1.3. настоящей Инструкции, совершенные им в порядке и в случаях, предусмотренных законодательством Российской Федерации, во исполнение нормативных актов Организации или договоров (соглашений) Организации с иными организациями или физическими лицами. Не считаются разглашением конфиденциальной информации действия сотрудника, совершенные им при наличии письменного разрешения или иного указания руководства Организации.

1.5. Меры по ограничению открытых публикаций конфиденциальной информации не могут быть использованы для сокрытия информации, связанной с:

- учредительными документами организации;
- документами, дающими право заниматься предпринимательской деятельностью (регистрационными удостоверениями, лицензиями, патентами и т.д.);
- сведениями о финансово-хозяйственной деятельности и иными сведениями, необходимыми для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему;
- документами о платежеспособности;
- сведениями о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;
- документами об уплате налогов и обязательных платежей;
- сведениями о загрязнении окружающей среды;
- сведениями о нарушении антимонопольного законодательства;
- сведениями о несоблюдении безопасных условий труда;
- сведениями о реализации продукции, причиняющей вред здоровью населения.

1.6. Предоставление конфиденциальной информации представителям контрольных, ревизионных, фискальных и следственных органов, народным депутатам, органам печати, радио, телевидения и т.п. допускается только с разрешения руководителя Организации.

1.7. Защита конфиденциальной информации предусматривает:

- определение конфиденциальной информации, и сроков ее защиты;
- систему допуска сотрудников Организации, частных и командированных лиц к конфиденциальной информации;
- обязанности лиц, допущенных к конфиденциальной информации;
- порядок работы с бумажными документами, содержащими конфиденциальную информацию;

- порядок работы с электронными документами, содержащими конфиденциальную информацию;
- обеспечение сохранности документов и дел (архивов) содержащих конфиденциальную информацию;
- принципы организации и проведения контроля за обеспечением установленного порядка при работе с конфиденциальной информацией;
- ответственность за разглашение конфиденциальной информации и утрату документов, содержащих конфиденциальную информацию.

1.8. Обязанности по конфиденциальному делопроизводству возлагаются на секретаря руководителя Организации (в части делопроизводства руководителя Организации), секретарей руководителей структурных подразделений Организации (в части делопроизводства структурных подразделений) и системного администратора корпоративной компьютерной сети (в части обеспечения работоспособности электронной системы делопроизводства).

1.9. Конфиденциальная информация должны находиться преимущественно в электронном виде и быть защищена электронными средствами защиты.

1.10. Входящие конфиденциальные бумажные документы секретарями переводятся в электронный вид, дальнейшая работа с данными документами происходит сотрудниками в электронном виде.

1.11. Работа сотрудников с конфиденциальными бумажными документами допускается в виде исключения с разрешения руководства Организации или руководства структурных подразделений в случае невозможности или нецелесообразности перевода документа в электронный вид.

1.12. После перевода конфиденциального входящего бумажного документа в электронный вид, данный документ, по решению руководства Организации или руководства структурного подразделения, уничтожается или, после отработки, определяется в соответствующее дело (архив).

1.13. Обмен конфиденциальными документами внутри организации, осуществляется, преимущественно, в электронном виде с использованием средств электронной защиты.

1.14. Порядок работы с электронными конфиденциальными документами определен в части 2 данной Инструкции.

1.15. Определение вида исходящего конфиденциального документа (электронного или бумажного) возлагается на исполнителя по согласованию с руководством Организации или руководством структурного подразделения.

1.16. Ответственность за организацию работы с конфиденциальной информацией, разработку и осуществление необходимых мер по сохранности конфиденциальной информации руководитель Организации возлагает на руководителей структурных подразделений, соответствующих должностных лиц Службы безопасности, секретарей и системного администратора закрытой корпоративной компьютерной сети.

2. Порядок работы с не документированной конфиденциальной информацией

2.1. Хранение, работа и архивирование любых электронных конфиденциальных документов (файлов) должно осуществляться с учётом требования ограничения несанкционированного доступа к ним третьих лиц способами, оговоренными настоящим разделом данной Инструкции.

2.2. Все персональные компьютеры, установленные на рабочих местах сотрудников, подключены к защищенной корпоративной компьютерной сети Организации (далее – сеть).

2.3. Каждый персональный компьютер оснащён стандартным набором программных средств, принятых для эксплуатации в Организации. Любые изменения в оснащении

персонального компьютера, подключённых к сети, должны быть санкционированы руководством структурного подразделения, согласованы с администратором сети и осуществлены уполномоченными специалистами Организации.

2.4. Вся конфиденциальная информация, имеющаяся в распоряжении сотрудника, должна храниться и обрабатываться на корпоративном файл-сервере Организации.

2.5. Первичный допуск сотрудника к работе на персональном компьютере, включенного в сеть осуществляется системным администратором сети по указанию руководства соответствующего структурного подразделения и включает в себя:

- ознакомление сотрудника с настоящей Инструкцией под роспись;
- инструктаж по порядку работы с программными средствами, принятыми для эксплуатации в Организации;
- получение сотрудником персонального ключа для шифрования данных;
- получение сотрудником персонального пароля для доступа к ресурсам корпоративного сервера и локальной вычислительной сети;
- получение адреса персонального почтового ящика корпоративной почты;
- получение внутреннего персонального ICQ номера.

2.6. Сотрудник, допущенный к работе с персональным компьютером, получает доступ:

- к персональному разделу на корпоративном файл-сервере («Личная» папка) для хранения и обработки электронных конфиденциальных документов (файлов) с предоставленной в его распоряжение для выполнения поставленных перед ним задач;
- к разделу с открытыми ключами сотрудников Организации;
- к персональному почтовому ящику корпоративной почты.

2.7. Все электронные конфиденциальные документы (файлы), должны храниться на корпоративном сервере одним из возможных способов:

- в личной папке сотрудника в защищённом на личном ключе виде;
- в личной папке сотрудника в защищённом на личном плюс один или несколько открытых ключей уполномоченных руководства сотрудников виде - в случае необходимости и по указанию руководства.

2.8. Все новые электронные конфиденциальные документы (файлы) должны создаваться только на файл-сервере в личной папке сотрудника.

2.9. Работа с электронными конфиденциальными документами (файлами), допускается только при условии расположения этих документов (файлов) на сервере способами оговоренными п.2.7.

2.10. В каждый конкретный момент времени в течение рабочего дня загруженными в персональный компьютер сотрудника должны быть только те электронные конфиденциальные документы (файлы), которые имеют непосредственное отношение к тому делу, которым занимается сотрудник в данный момент времени. При этом все другие конфиденциальные документы (файлы), должны находиться на сервере в виде согласно п.2.7.

2.11. Загрузка (открытие), сверх действительно необходимого количества, электронных конфиденциальных документов (файлов) на персональных компьютерах сотрудников запрещается.

2.12. В течение рабочего дня ставшие ненужными в текущей работе (отработанные) электронные конфиденциальные документы (файлы) подлежат незамедлительному закрытию (сохранению на файл-сервер).

2.13. С целью недопущения переполнения сетевых дисков, выявленные в течение дня ненужные файлы (старые версии файлов и т.д.) подлежат безусловному незамедлительному уничтожению.

2.14. Уничтожение электронных конфиденциальных документов (файлов) с сетевых дисков корпоративного файл-сервера осуществляется стандартными средствами операционной системы – команда «Удалить» контекстного меню. Уничтожение электронных конфиденциальных документов (файлов) с любых иных носителей должно осуществляться только с помощью утилиты Wipe специально предназначенной для уничтожения файлов без возможности их последующего восстановления.

2.15. Обмен электронными конфиденциальными документами (файлами) между сотрудниками находящимися в офисе осуществляется в зашифрованном виде одним из способов, используя сервис корпоративной почты.

2.16. Обмен электронными конфиденциальными документами (файлами) между сотрудниками, находящимися вне офиса Организации (командировки) осуществляется путем обмена зашифрованной почтой через корпоративные почтовые ящики сотрудников.

2.17. Порядок обращения с конфиденциальным бумажным документом, полученным в результате распечатки электронного конфиденциального документа, регламентируется соответствующими разделами данной Инструкции.

2.18. В случае прихода (ожидания) посетителя к сотруднику, в персональный компьютер этого сотрудника могут быть загружены только те электронные конфиденциальные документы (файлы), относящиеся к делу этого посетителя. Загружать в персональный компьютер и/или работать с электронными конфиденциальными документами (файлами), не относящимися к делу присутствующего посетителя - запрещается.

2.19. Сотруднику, работающему с электронными конфиденциальными документами (файлами) категорически запрещается:

- оставлять без присмотра персональный компьютер с разрешённым доступом к личной папке;
- сообщать, кому бы то ни было, свой персональный пароль доступа в закрытую корпоративную компьютерную сеть Организации;
- сообщать, кому бы то ни было, пароль доступа к своему персональному ключу PGP;
- оставлять посетителя в кабинете одного при включенном в защищенную корпоративную сеть компьютере;
- осуществлять хранение/обработку личных файлов (данных, не имеющих отношения к выполнению функциональных обязанностей, а именно: файлы mp3, игры, картинки, личные фотографии и т.д.) на сетевых дисках корпоративного сервера;
- использовать съёмные носители - дискеты, ZIP диски, магнитооптика и т.д. – для обмена между сотрудниками и хранения электронных конфиденциальных документов (файлов);
- самовольно, без согласования с администратором сети, изменять аппаратную конфигурацию и настройки программного обеспечения персональных компьютеров, подключенных к сети.

2.20. Сотрудник, работающий с электронными конфиденциальными документами (файлами) обязан:

- выполнять требования администратора сети в рамках установленного регламента эксплуатации сети и требований настоящей Инструкции (технический перерыв, устра-

нение выявленных нарушений хранения/обработки данных, профилактические работы на оборудовании сети). Несоблюдение требований настоящего пункта может привести к необратимой потере данных, ответственность за которую возлагается на самих сотрудников.

- при убытии в отпуск/командировку предоставить имеющиеся у него конфиденциальные электронные документы (файлы), которые могут понадобиться в его отсутствие (определяется руководителем), в распоряжение уполномоченного руководителем сотрудника в зашифрованном на открытом ключе этого сотрудника виде;
- ежедневно в конце рабочего дня производить «зачистку» локального диска своего персонального компьютера путём запуска соответствующей процедуры (ярлык «До свидания!» на рабочем столе Windows);
- еженедельно производить ревизию своей личной папки, размещённой на корпоративном файл-сервере, с целью выявления и уничтожения конфиденциальных электронных документов (файлов) ставших ненужными.

3. Определение конфиденциальной информации и обозначение бумажных документов, содержащих конфиденциальную информацию, и сроков ее защиты

3.1. На документах и делах (архивах), содержащих конфиденциальную информацию, проставляется гриф "Конфиденциально", а также номера экземпляров. Гриф и номера экземпляров, проставляются в правом верхнем углу каждой страницы документа.

3.2. Необходимость проставления грифа "Конфиденциально" определяется исполнителем документа и утверждается руководством структурного подразделения, в соответствии с Перечнем, указанным в п. 1.2. настоящей Инструкции.

3.3. На наиболее важных конфиденциальных документах, с содержанием которых необходимо ознакомить строго ограниченный круг лиц, и документах, подлежащих направлению (передаче) лично адресатам, проставляется ограничительная пометка «Лично». При необходимости в документе указывается, кто из должностных лиц должен (может) быть ознакомлен с ним.

3.4. На обратной стороне последнего листа каждого экземпляра печатается разметка, в которой указывается: количество отпечатанных экземпляров, регистрационный номер, фамилия исполнителя и его телефон, дата, и срок защиты (регистрационный номер проставляется на каждом листе документа).

3.5. Срок защиты конфиденциальной информации, содержащейся в документе, определяется в каждом конкретном случае исполнителем и утверждается руководством структурного подразделения, в виде конкретной даты или в виде пометок: "до заключения контракта", "бессрочно" и т.п. и своей подписи.

3.6. Основанием для снятия грифа "Конфиденциально" является решение руководства структурного подразделения, оформляемое актом, утвержденным руководителем организации. Один экземпляр акта вместе с делами передается в архив организации.

3.7. Гриф "Конфиденциально" после оформления его снятия (п. 2.4) погашается штампом или записью от руки с указанием даты и номера акта, послужившего основанием для его снятия. Аналогичные отметки вносятся в описи дел (архивов).

4. Организация работы с бумажными документами, имеющих гриф «Конфиденциально»

4.1. Все входящие, исходящие и внутренние бумажные документы, имеющие гриф "Конфиденциально", подлежат обязательной регистрации у соответствующих секретарей в специальных регистрационных журналах и учитываются по количеству листов, а издания - поэкземплярно.

4.2. Права на информацию, порядок пользования ею, сроки ограничения на публикацию могут оговариваться дополнительно в тексте документа, его реквизитах или резолюциях.

4.3. Отсутствие грифа "Конфиденциально" и предупредительных оговорок в тексте и реквизитах означает свободную рассылку и предполагает, что автор информации и лицо, подписавшее или утвердившее документ, предусмотрели возможные последствия от свободной рассылки и несут за это ответственность.

4.4. Вся входящая корреспонденция, имеющая гриф "Конфиденциально" (или другие соответствующие этому понятию грифы, например, "секрет предприятия, "тайна предприятия" и др.) вскрывается сотрудниками организации, имеющими соответствующий допуск и которым поручена работа с этими материалами. При этом проверяется количество листов и экземпляров, а также наличие указанных в сопроводительном письме приложений. При обнаружении отсутствия в конвертах (пакетах) указанных документов составляется акт в двух экземплярах: один экземпляр акта направляется отправителю.

4.5. На рассмотрение руководства Организации передаются все конфиденциальные бумажные документы, адресованные руководству Организации, документы, по которым только руководство Организации может назначить исполнителя, а также в случае, если документ адресован конкретному сотруднику, а последний не имеет права доступа к данной категории документов.

4.6. Учет бумажных документов с грифом "Конфиденциально" ведется в регистрационных журналах отдельно от учета другой служебной документации не имеющей ограничения по доступу. Листы регистрационных журналов нумеруются, прошиваются и опечатываются.

4.7. Проекты (черновики) конфиденциальных бумажных документов исполнителями составляются только в электронном виде с использованием электронных средств защиты или в специальных персональных тетрадях, указанных в пункте данной Инструкции.

4.8. Конфиденциальные бумажные документы составляются в строго ограниченном количестве экземпляров. Исходящие документы составляются, как правило, в двух экземплярах, а внутреннего обращения – в одном.

4.9. Движение бумажных документов с грифом "Конфиденциально" осуществляется через соответствующих секретарей и только с помощью персонального реестра (с обязательной подписью исполнителя, получившего документ) и своевременно отражается в регистрационных журналах.

4.10. На зарегистрированном входящем документе с грифом, ограничивающим доступ к информации, должен быть проставлен штамп с указанием наименования организации, регистрационный номер документа и дата его поступления.

4.11. Отпечатанные и подписанные исходящие документы с грифом «Конфиденциально» передаются для регистрации секретарю руководителя организации (в случае, если исходящий документ подписан руководством организации) или секретарю руководителя структурного подразделения (в случае если исходящий документ подписан руководством структурного подразделения).

4.12. В случае, если исходящий бумажный конфиденциальный документ рассылается в несколько адресов, рассылка производиться на основании подписанных руководством Организации или руководством структурных подразделений разнарядок с указанием учетных номеров отправляемых экземпляров. Отправка по Москве и в ближайшие регионы осуществляется только с помощью курьеров организации. В отдаленные регионы отправка данных документов осуществляется с помощью органов спецсвязи или фельдсвязи.

4.13. Размножение бумажных документов с грифом "Конфиденциально" на копировально-множительной технике производится только у соответствующих секретарей на основании вышеуказанных разнарядок или иных разрешений руководства Организации или руководителей структурных подразделений.

Размноженные документы с грифом "Конфиденциально" (копии, тираж) должны быть полистно подобраны, пронумерованы поэкземплярно и, при необходимости, сброшюрованы (сшиты). Нумерация дополнительно размноженных экземпляров, производится от последнего номера, ранее учтенных экземпляров этого документа.

После размножения на последнем листе оригинала (подлинника) проставляется запись: " Регистрационный номер _____. Дополнительно размножено _____ экз., на _____ листах текста. Должность, Ф.И.О. лица, разрешившего размножение. Дата. Подпись.

Одновременно делается отметка об этом в соответствующих регистрационных журналах.

4.14. Бумажные документы с грифом "Конфиденциально" после исполнения группируются в отдельные дела в хронологическом порядке.

4.15. Снятия рукописных, машинописных, микро – ксеро и фотокопий, электрографических и др. копий, а также производство выписок из документов с грифом «Конфиденциально» сотрудниками Организации производится по разрешению руководства Организации или руководства структурных подразделений. Данные выписки должны делаться в специальные персональные тетради, имеющие гриф «Конфиденциально», регистрационные номера, пронумерованные страницы, которые прошиты и скреплены печатью организации.

4.16. Печатание документов, содержащих конфиденциальную информацию на бумажные носители разрешается у секретарей или непосредственно на рабочем месте исполнителя.

4.17. Уничтожение бумажных документов с грифом "Конфиденциально" производится комиссией в составе не менее трех человек с составлением соответствующего акта, при этом один человек должен быть сотрудником Службы безопасности.

5. Порядок обеспечения сохранности документов и дел (архивов), содержащих конфиденциальную информацию

5.1. Все документы, и дела (архивы) с документами имеющими гриф "Конфиденциально" должны храниться в офисных помещениях в надежно запираемых и опечатываемых сейфах (металлических шкафах). Помещения должны отвечать требованиям внутри объектного режима, обеспечивающего физическую сохранность находящейся в них документации.

5.2. Дела (архивы) с документами имеющими гриф "Конфиденциально", выдаются секретарями под роспись в регистрационном журнале и подлежат возврату сотрудниками в тот же день. При необходимости, с разрешения руководства структурного подразделения, они могут находиться у сотрудника в течении срока, необходимого для выполнения задания, при условии полного обеспечения их сохранности и соблюдения правил хранения.

5.3. С документами (электронными и бумажными) с грифом "Конфиденциально" разрешается работать только в офисных помещениях Организации. Для работы вне офисных помещений необходимо разрешение руководства Организации или руководства структурного подразделения.

5.4. Во время перерывов в работе, связанных с выходом из своего офисного помещения, запрещается оставлять конфиденциальные документы на столах, в незапертых ящиках столов. В случае нахождения в офисном помещении посетителей или иных лиц, не имеющих допуск к конфиденциальным бумажным документам, все конфиденциальные документы должны быть убраны в сейфы (металлические шкафы).

5.5. Изъятия из дел (архивов) или перемещение бумажных документов с грифом "Конфиденциально" из одного дела (архива) в другое без санкции руководства Организации или руководства структурных подразделений запрещается.

5.6. Смена секретарей, ответственных за учет и хранение документов, дел (архивов) с грифом "Конфиденциально", оформляется распоряжением руководства Организации или руководства структурных подразделений. При этом составляется акт приема-передачи этих материалов, утверждаемый соответствующим руководством.

6. Порядок допуска к конфиденциальным сведениям

6.1. Допуск сотрудников к конфиденциальным сведениям осуществляется руководством Организации и оформляется соответствующим решением в письменной форме.

6.2. Руководители структурных подразделений обязаны обеспечить систематический контроль за допуском к конфиденциальным сведениям только тех лиц, которым они необходимы для выполнения функциональных обязанностей.

6.3. К конфиденциальным сведениям допускаются лица, личные и деловые качества которых обеспечивают их способность хранить конфиденциальную информацию, и только после оформления письменного обязательства по сохранению конфиденциальной информации.

6.4. Допуск сотрудников к работе с делами (архивами), в которых хранятся конфиденциальные документы осуществляется согласно оформленному на внутренней стороне обложки дела (архива) или на отдельном листе списку допущенных сотрудников за подписью руководства Организации, а к документам - в соответствии с указаниями, содержащимися в резолюциях руководства Организации или руководства структурных подразделений.

6.5. Представители сторонних организаций и частные лица могут быть допущены к ознакомлению и работе с документами и делами (архивами) с грифом "Конфиденциально" только с разрешения руководства Организации.

6.6. Выписки из документов, содержащих сведения с грифом "Конфиденциально", производятся в специальных тетрадях, определенных в пункте настоящей Инструкции. После окончания работы они высылаются в адрес той организации, которая будет указана данным представителем.

7. Контроль за выполнением требований внутри объектового режима при работе с конфиденциальными сведениями

7.1. Под внутри объектовым режимом при работе с конфиденциальными документами подразумевается соблюдение условий работы, исключающих возможность утечки информации о конфиденциальных сведениях.

7.2. Контроль за соблюдением указанного режима осуществляется в целях изучения и оценки состояния сохранности конфиденциальной информации, выявления и установления причин недостатков, и выработки предложений по их устранению.

7.3. Контроль за обеспечением режима при работе с конфиденциальными сведениями осуществляют соответствующие сотрудники Службы безопасности и руководители структурных подразделений путем текущих и внеплановых проверок.

7.4. При проведении проверок создается комиссия, которая комплектуется из сотрудников Службы безопасности и сотрудников организации в составе не менее двух человек, допущенных к работе с материалами, имеющими гриф «Конфиденциально».

7.5. Участие в проверке не должно приводить к необоснованному увеличению осведомленности в этих сведениях, а также затруднять работу сотрудников Организации.

7.6. Плановые проверки проводятся не реже одного раза в год на основании распоряжения руководства Организации.

7.7. Внеплановые проверки проводятся при наличии признаков утечки конфиденциальной информации или по иной необходимости на основании распоряжения руководителя Организации по согласовании со Службой безопасности.

7.8. Проверяющие имеют право знакомиться со всеми документами и иными материалами, имеющими отношение к проверяемым вопросам, а также проводить беседы, консультироваться со специалистами и исполнителями, требовать представления письменных объяснений, справок и отчетов по всем вопросам, входящим в компетенцию комиссии.

7.9. При проверках может присутствовать руководство структурного подразделения.

7.10. По результатам проверок составляется акт или справка с отражением в нем наличия документов, состояния работы с материалами, имеющими гриф "Конфиденциально", выявленных недостатков и предложений по их устранению. Акт подписывается начальником Службы безопасности и утверждается руководством Организации.

7.11. При выявлении случаев утраты документов или разглашения конфиденциальных сведений ставятся в известность руководитель организации и начальник Службы безопасности. Для расследования указанных случаев распоряжением руководителя Организации создается комиссия, которая определяет соответствие содержания утраченного документа проставленному грифу "Конфиденциально" и выявляет обстоятельства утраты (разглашения), а также предложения по минимизации потерь, связанных утратой документа или разглашением конфиденциальной информации. По результатам работы комиссии составляется акт.

8. Обязанности сотрудников Организации, работающих с конфиденциальными сведениями и их ответственность за ее разглашение

8.1. Сотрудники организации, допущенные к конфиденциальными сведениям, несут ответственность за точное выполнение требований, предъявляемых к ним в целях обеспечения сохранности указанных сведений.

8.2. До получения доступа к работе, связанной с конфиденциальной информацией, им необходимо изучить настоящую Инструкцию под роспись и заключить письменное обязательство о сохранении конфиденциальной информации, оформленное в виде договора.

8.3. Сотрудники организации, допущенные к конфиденциальной информации должны:

- знать и соблюдать требования настоящей Инструкции;
- хранить конфиденциальную информацию, в том числе не сообщать конфиденциальные сведения друзьям и членам своей семьи. О ставших им известной утечке сведений, составляющих конфиденциальную информацию, а также об утрате документов с грифом «Конфиденциально», немедленно сообщать своему руководителю структурного подразделения и в Службу безопасности;
- предъявлять для проверки по требованию комиссии по проверке конфиденциального делопроизводства и представителей Службы безопасности все числящиеся за ним материалы, содержащие конфиденциальную информацию, а в случае нарушения установленных правил работы с ними представлять соответствующие объяснения в устном и письменном виде;
- знакомиться только с теми документами и выполнять только те работы, к которым они допущены в соответствии с функциональными обязанностями и в соответствии с дополнительными задачами, возложенными на них руководством;
- строго соблюдать правила пользования и сохранности документов, имеющих гриф «Конфиденциально». Не допускать их необоснованной рассылки;
- выполнять требования внутри объектного режима, определяемые Службой безопасности, исключающие возможность ознакомления с материалами, содержащими конфиденциальную информацию, посторонних лиц, включая и сотрудников организации, не имеющих к указанным материалам прямого отношения.
- при ведении деловых переговоров с представителями сторонних организаций или частными лицами ограничиваться выдачей минимальной информации, действительно необходимой для их успешного завершения;
- при временном убытии (в отпуск, командировку, на учебу, лечение и т.д.) проверять наличие числящихся за ним конфиденциальных документов. Документы, которые подлежат исполнению или могут потребоваться в работе, передавать другому сотруднику по указанию руководства организации или руководства структурного подразделения. При прекращении трудовых или иных договорных отношений с Организацией, сотрудник обязан сдать все числящиеся за ним конфиденциальные документы;
- исключить использование конфиденциальных сведений в свою личную пользу, а также исключить деятельность, которая может быть использована конкурентами в ущерб организации.

8.4. Ответственность за разглашение конфиденциальных сведений, и утрату документов, содержащих такие сведения устанавливается в соответствии с Уголовным кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Кодексом Российской Федерации об административных правонарушениях, Кодексом законов о труде Российской Федерации и иным действующим законодательством.

Вставьте ниже заполненный документ

Практическая работа № 14
«Составление заявления на предоставление временного доступа»

Задание

1. В верхнем колонтитуле укажите свою фамилию и инициалы.
2. Составьте и оформите заявление на предоставление временного доступа к конфиденциальной информации **с учетом данных Вашей организации**.

Заявление должно обязательно содержать следующие элементы:
Сведения об адресате и заявителе (т.н. «шапка»).
Наименование документа.
Формулировка просьбы.
Дата подачи.
Подпись заявителя.

При формулировке просьбы необходимо указать причину, по которой необходимо предоставить временный доступ к конфиденциальной информации, это может быть, например, участие в работе на новым проектом, в этом случае нужно указать название или тематику проекта.

Правила оформления реквизитов приведены в 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 скриншот заявления

Практическая работа № 15
«Разработка проекта приказа на временный доступ»

Задание

1. В верхнем колонтитуле укажите свою фамилию и инициалы.
2. Разработайте и оформите Приказ о предоставлении временного доступа к конфиденциальной информации с **учетом данных Вашей организации**.

При формулировке текста приказа необходимо указать причину, по которой необходимо предоставить временный доступ к конфиденциальной информации, это может быть, например, участие в работе на новым проектом, в этом случае нужно указать название или тематику проекта.

Приказ должен соответствовать заявлению, которое было создано в предыдущей практической работе.

Приказ должен быть оформлен в соответствии с требованиями по оформлению организационно-распорядительных документов.

Правила оформления реквизитов приведены в 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 скриншот приказа.

Практическая работа № 16
«Разработка журналов учета доступа и использования КИ»

Задание

1. В верхнем колонтитуле укажите свою фамилию и инициалы.
2. Разработайте и оформите журнал учета доступа и использования КИ с учетом данных Вашей организации. Журнал необходимо расположить на отдельной странице, которая имеет альбомную ориентацию.
3. Заполните журнал пятью записями с учетом, что часть документов уже возвращена.

Форма журнала:

ЖУРНАЛ (КАРТОТЕКА)
учета работников, включая работников других организаций, получающих в пользование конфиденциальную документированную информацию

Дата выдачи документа	Номер записи	Наименование документа	Номер и дата документа	Наименование структурного подразделения или иной организации	Должность, фамилия, имя, отчество	Цель получения	Основание получения	Расписка в получении	Дата возврата	Подтверждение возврата (подпись лица, ответственного за выдачу документов)	Примечание

Вставьте заполненный журнал

Практическая работа № 17
«Подготовка памятки для персонала по организации работы с конфиденциальной информацией сотрудника при увольнении»

Задание

1. В верхнем колонтитуле укажите свою фамилию и инициалы.
2. Используя материал лекций и ресурсы сети Интернет, составьте памятку для персонала по организации работы с конфиденциальной информацией сотрудника при увольнении.

Памятка должна содержать перечень действий, которые обязан выполнить сотрудник, который принял решение об увольнении.

Памятка должна быть оформлена общем бланке организации.

Требования по оформлению:

Основной текст - шрифт Times New Roman, 12 пт, междустрочный интервал 1,15, отступ красной строки 1, 25 см, выравнивание по ширине страницы.

Заголовок - шрифт Times New Roman, 12 пт, полужирный, междустрочный интервал 1,15, интервал после 24 пт, выравнивание по центру страницы.

Вставить памятку

Практическая работа № 18
«Разработка инструкции по учету, обработке, хранению, передаче, использованию различных носителей конфиденциальной информации»

Задание

1. В верхнем колонтитуле укажите свою фамилию и инициалы.
2. Составьте и оформите инструкцию по организации учета, использования, передачи и уничтожения электронных носителей персональных данных

И ДРУГОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ **с учетом данных Вашей организации**.

При оформлении инструкции необходимо выполнить следующие требования:

1. Инструкция оформляется на бланке организации.
2. Инструкция должна быть утверждена руководителем организации
3. Инструкция должна быть согласована экспертной комиссией по защите конфиденциальной информацией.
4. Инструкция должна быть подписана составителем, которым является руководитель службы безопасности (реквизит подпись располагается на последнем листе инструкции до приложений).
5. Инструкция должна обязательно содержать **лист ознакомления** сотрудника с инструкцией. Лист ознакомления должен располагаться до приложений.

Правила оформления грифов и реквизитов приведены в 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

Шаблон (**шаблон не изменять!**):

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ УЧЕТА, ИСПОЛЬЗОВАНИЯ, ПЕРЕДАЧИ И УНИЧТОЖЕНИЯ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ И ДРУГОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

1. Общие положения

1.1. Настоящая Инструкция устанавливает основные требования к организации учета, использования, передачи и уничтожения электронных носителей информации (далее - носители), предназначенных для обработки персональных данных и иной конфиденциальной информации в Общество с ограниченной ответственностью «…» (далее – ООО «…»).

1.2. К электронным носителям информации относятся: CD- и DVD-диски, USB флеш-диски, накопители на жестких магнитных дисках и др.

1.3. Ответственность за организацию учета, использования, передачи и уничтожения носителей, предназначенных для обработки и хранения персональных данных и иной конфиденциальной информации, затирание (удаление) информации возлагается на администратора информационной безопасности.

1.4. Положения данной инструкции обязательны для выполнения всеми сотрудниками ООО «…»), которые в ходе выполнения своих должностных обязанностей используют носители персональных данных и иной конфиденциальной информации, а также имеющими допуск к обработке персональных данных и иной конфиденциальной информации.

I2. Учёт и хранение электронных носителей информации

2.1. Учёту подлежат все носители информации, находящиеся в распоряжении ООО «…».

2.2. Носители учитываются в специальном «Журнале регистрации и учета электронных носителей персональных данных и иной конфиденциальной информации» (Приложение №1) в котором производится непосредственно регистрация и учёт носителей.

2.3. Регистрация и учет носителей информации осуществляется администратором информационной безопасности.

2.4. Учётный номер носителя состоит из сокращенного наименования подразделения (отдела) и порядкового номера по журналу регистрации через дефис и грифа информации (например: уч. № ОБ-1/К, где ОБ – отдел бухгалтерии, 1 – порядковый номер в журнале, К – «Конфиденциально»).

2.5. Каждый носитель информации, применяемый при обработке информации на средствах вычислительной техники (далее - СВТ), должен иметь гриф конфиденциальности, соответствующий записанной на нём информации. Исключается хранение на одном носителе информации разных грифов конфиденциальности, а также хранение информации, имеющей разные цели обработки.

2.6. Для съемных носителей информации реквизиты наносятся непосредственно на носитель (корпус). Если невозможно маркировать непосредственно носитель (корпус), то применяется маркировка упаковки, в которой хранится носитель или другие доступные способы маркировки (бирки, брелоки и т.п.). Надпись реквизитов делается разборчиво и аккуратно. На дискеты и футляры носителей допускается наклеивать заранее заготовленную этикетку.

2.7. Каждому носителю в журнале должна соответствовать отдельная строка.

2.8. Накопители на жестких магнитных дисках (НЖМД) в серверах и системных блоках компьютеров учитываются в паспорте (формуляре) на поставляемое оборудование с указанием марки носителя информации и его серийного номера.

2.9. Хранение носителей информации осуществляется в условиях (закрываемые шкафы, сейфы и т.п.), исключающих возможность хищения, приведения в негодность или уничтожения содержащейся на них информации.

2.10. О фактах утраты носителей необходимо незамедлительно докладывать руководителю своего структурного подразделения**.**

2.11. Администратор информационной безопасности не реже одного раза в год осуществляет проверку условий хранения носителей персональных данных и иной конфиденциальной информации.

3. Выдача/сдача и передача носителей

3.1. Выдача носителей сотрудникам осуществляется администратором информационной безопасности под подпись с отметкой в «Журнале выдачи/сдачи электронных носителей персональных данных и иной конфиденциальной информации» (Приложение № 2). Факт сдачи носителя регистрируется аналогичным образом.

3.2. Носители, как правило, выдаются только непосредственно на время работы с данным носителем и сдаются сотрудником администратору информационной безопасности сразу по завершению таких работ.

3.3. Носители, которые выдаются сотруднику, должны пройти проверку на отсутствие записанной на ней информации. В случае наличия какой-либо информации на выдаваемом носителе, администратор информационной безопасности обязан удалить **(**затереть) информацию согласно п. 4. настоящей инструкции.

3.4. В случае повреждения носителей, содержащих персональные данные и (или) иную конфиденциальную информацию, сотрудник, в пользовании которого они находятся, обязан сообщить о случившемся руководителю своего структурного подразделения (отдела) и администратору информационной безопасности.

3.5. При передаче в другие организации носители информации должны, по возможности, быть упакованы в пакет/конверт, обеспечивающий сохранность (работоспособность) передаваемого носителя. При этом носители информации передаются с сопроводительным письмом, в котором указывается, какая информация содержится на данном носителе, а для подтверждения достоверности информации прилагается таблица с реквизитами файлов (допускается прикладывать скриншот окна архиватора). Данное передвижение (передача) носителей персональных данных и иной конфиденциальной информации регистрируется в «Журнале передачи носителей персональных данных и иной конфиденциальной информации» (Приложение 3), где делается отметка об отправке (куда отправлен (реквизиты адресата), исходящий номер сопроводительного письма, дата отправки, способ отправки (курьер, заказная почта и т.п.)) и отметка о получении (номер «Уведомления о вручении» или «Накладной»). В случае если передача носителей осуществляется лично сотрудником ООО «Гарант», то у адресата, необходимо взять расписку о получении носителя (Приложение 4).

3.6. Для исключения утечки информации, находящейся на жестких дисках компьютеров, при необходимости ремонта компьютера в сервисном центре, жесткий диск с компьютера демонтируется и компьютер отправляется в ремонт без жесткого диска. При необходимости диагностирования самого жесткого диска информация должна быть предварительно скопирована на резервный носитель и затем стёрта с направляемого в ремонт винчестера с использованием специальных средств (сертифицированные программные или программно-аппаратные средства защиты информации, обеспечивающие невозможность восстановления информации), либо путём полного трехкратного его форматирования. Если невозможно произвести данные действия (поломка жесткого диска или ПЭВМ), то отправка такой ПЭВМ в ремонт возможна только по письменному разрешению руководителя организации.

4. Порядок уничтожения носителей, затирания информации на носителях

4.1. Уничтожение носителей информации, пришедших в негодность или утративших практическую ценность, производится путем их физического разрушения без возможности дальнейшего восстановления.

4.2. Перед уничтожением носителя вся информация с него должна быть стерта (уничтожена) путем использования специальных средств (сертифицированные программные или программно-аппаратные средства защиты информации, обеспечивающие невозможность восстановления информации), либо путём полного трехкратного его форматирования, если это позволяют физические принципы работы носителя.

4.3. Уничтожение носителей, затирания (уничтожении) информации с носителей производиться комиссией из 3 человек, назначенной приказом руководителя ООО «…»). В состав комиссии должен входить администратор информационной безопасности.

4.4. По факту уничтожения носителей, а также затирания (уничтожения) информации на носителях, комиссией составляется Акт (Приложение № 5). В Акте указываются учётные номера носителей, характер уничтожаемой (затираемой) информации, причина уничтожения носителя (затирания информации на нем). Реквизиты Акта заносятся председателем данной комиссии в графу «Сведения об уничтожении» «Журнала регистрации и учета электронных носителей персональных данных и иной конфиденциальной информации». Подписанный Акт храниться у администратора информационной безопасности.

Приложение 1
к Инструкции по организации учета,
использования, передачи и уничтожения
электронных носителей
конфиденциальной информации
и персональных данных

ООО «…»

Журнал №__
регистрации и учета электронных носителей персональных данных и иной конфиденциальной информации

с «__»_____202_ г.
по «__»_____202_ г.

ФИО и должность ответственного за ведение журнала:
_____

Журнал составлен на ____ листах

№ п/п	Регистрационный номер электронного носителя	Вид (тип, модель) электронного носителя	Характер информации, которая будет содержаться на носителе	Дата регистрации электронного носителя	ФИО лица, регистрирующего носитель	Подпись лица, регистрирующего носитель	Сведения об уничтожении носителя (№ акта, дата)

1	2	3	4	5	6	7	8

Приложение 2
к Инструкции по организации учета,
использования, передачи и уничтожения
электронных носителей
конфиденциальной информации
и персональных данных

ООО «…»

Журнал №__
выдачи/сдачи электронных носителей персональных данных и иной конфиденциальной информации

с «__»_____202_ г.
по «__»_____202_ г.

ФИО и должность ответственного за ведение журнала:
_____

Журнал составлен на ____ листах

Дата	Время	Регистрационный номер электронного носителя	Сдал		Принял	
			ФИО, должность	Подпись	ФИО, должность	подпись
1	2	3	4	5	6	7

Приложение 3
к Инструкции по организации учета,
использования, передачи и уничтожения
электронных носителей
конфиденциальной информации
и персональных данных

ООО «…»

Журнал №__
передачи носителей персональных данных и иной конфиденциальной информации

с «__»_____202_ г.
по «__»_____202_ г.

ФИО и должность ответственного за ведение журнала:
_____

Журнал составлен на ____ листах

Дата	Регистрационный номер электронного носителя	Характер информации, содержащейся на передаваемом носителе	Исходящий номер сопроводительного письма	Адресат (название организации, отдел, должность, ФИО и т.п.)	Способ передачи/отправки носителя (лично, курьер, заказная почта)	Отправитель (лицо, записавшее информацию на носитель)		Отметка о доставке (дата, реквизиты документа, подтверждающие доставку)
						ФИО, должность	Подпись	
1	2	3	4	5	6	7	8	9

Приложение 4
к Инструкции по организации учета,
использования, передачи и уничтожения
электронных носителей
конфиденциальной информации
и персональных данных

№_____
заполняется отправителем

Расписка
(составлена в двух экземплярах, по одному для каждой из сторон)

«___»_____ 202_ г. г. Санкт-Петербург

Настоящим подтверждаю получение электронного носителя информации (Регистрационный номер электронного носителя_____) с сопроводительным письмом (Исходящий номер сопроводительного письма _____) от

Название организации: ООО «…» _____
Должность и ФИО представителя организации:_____
_____

Сведения о получателе:

Название организации:_____
Должность и ФИО получателя:_____
_____

«___»_____ 202_ г. _____/_____/
подпись получателя расшифровка

Приложение 5
к Инструкции по организации учета,
использования, передачи и уничтожения
электронных носителей
конфиденциальной информации
и персональных данных

ООО «…»

АКТ № ____
о затирании/уничтожении персональных данных и иной конфиденциальной информации/электронных носителей

«____»_____202_ г. г. Санкт-Петербург

Комиссия в составе:
Председатель:_____ (ФИО)
Члены комиссии: _____ (ФИО)
_____ (ФИО)

составила настоящий Акт о том, что в ее присутствии уничтожены следующие электронные носители персональных данных и иной конфиденциальной информации/ информация на следующих электронных носителях

Регистрационный номер электронного носителя	Вид (тип, модель) электронного носителя	Характер информации, которая содержится на носителе	Причина	Способ уничтожения (физическое разрушение, форматирование, с использованием специальных программных средств (каких))
1	2	3	4	5

Председатель комиссии: _____(ФИО)
подпись

Члены комиссии: _____(ФИО)
подпись

_____(ФИО)
подпись

Отметку в «Журнал регистрации и учета электронных носителей персональных данных и иной конфиденциальной информации» произвел администратор информационной безопасности_____(ФИО)_____.
подпись

Практическая работа № 19
«Заполнение документов по учету, обработке, хранению, передаче, использованию различных носителей конфиденциальной информации»

Задание

1. В верхнем колонтитуле укажите свою фамилию и инициалы.
2. Ознакомьтесь с предложенной ситуацией:

Вашей организацией был приобретён USB флеш накопитель, модель TRANSCEND Jetflash 790 256Гб, USB3.0, черный.

В соответствии с установленными в организации принципами формирования регистрационных номеров носителю был присвоен регистрационный номер ОП-48/К (ОП – отдел продаж, 48 – порядковый номер, К - конфиденциально), носитель был зарегистрирован 06.04.2020.

07.04.2020 носитель был выдан менеджеру отдела продаж Николаеву Александру Михайловичу.

Николаев А.М. записал на носитель проект нового договора продаж и предал через курьера, Антипченко Андрея Евгеньевича, Вашей организации носитель в юридическую консультацию на проверку.

Данные юридической консультации: 191186, Санкт-Петербург, ул. Большая Конюшенная, дом 29, юрист Викторов Сергей Борисович.

Юрист получил носитель в день оправки.

После проверки проекта договора, юрист записал на носитель скорректированный вариант, вызвал того же курьера, который привез носитель Николаеву А.М. 13.04.2020.

После получения носителя Николаев А.М. переписал всю необходимую информацию на свой рабочий компьютер и сдал носитель 14.04.2020.

Во избежании возможной утечки конфиденциальной информации все данные на указанном носителе были затерты.

3. Составьте и оформите все необходимые документы по учету, обработке, хранению, передаче, использованию различных носителей конфиденциальной информации **с учетом данных Вашей организации и в строгом соответствии с Инструкцией по учету, обработке, хранению, передаче, использованию различных носителей конфиденциальной информации**.

При создании документов ситуация рассматривается только с точки зрения Вашей организации.

Оформление документов должно соответствовать ГОСТу 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 скриншоты документов:

Практическая работа № 20
«Решение ситуационных задач»

Задание

1. В верхнем колонтитуле укажите свою фамилию и инициалы.
2. Посмотрите внимательно на фотографию ниже:

3. Какие требования по обеспечению защиты конфиденциальной информации в ходе проведения совещаний/переговоров по конфиденциальным вопросам нарушены?

Ответ:

4. Какие действия необходимо предпринять сотрудникам подразделения безопасности после окончания совещания, показанного на фотографии, чтобы снизить риск утечки конфиденциальной информации?

Ответ:

Практическая работа № 21
«Разработка инструкции по защите конфиденциальной информации при работе с зарубежными партнерами»

Задание

1. В верхнем колонтитуле укажите свою фамилию и инициалы.

2. Составьте и оформите инструкцию по защите конфиденциальной информации при работе с зарубежными партнерами **с учетом данных Вашей организации**.

При оформлении инструкции необходимо выполнить следующие требования:

1. Инструкция оформляется на бланке организации.
2. Инструкция должна быть утверждена руководителем организации
3. Инструкция должна быть согласована экспертной комиссией по защите конфиденциальной информацией.
4. Инструкция должна быть подписана составителем, которым является руководитель службы безопасности.
5. Инструкция должна обязательно содержать **лист ознакомления** сотрудника с инструкцией. Лист ознакомления должен располагаться в конце инструкции после реквизита подпись.

Правила оформления грифов и реквизитов приведены в 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

Шаблон (**шаблон не изменять!**):

ИНСТРУКЦИЯ
ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПРИ РАБОТЕ
С ЗАРУБЕЖНЫМИ ПАРТНЕРАМИ

1. Общие положения

1.1. Настоящая инструкция определяет порядок работы с зарубежными партнерами. Положениями настоящей инструкции необходимо руководствоваться также и при контактах с представителями совместных предприятий и с представителями конкурирующих фирм и организаций.

1.2. При работе с зарубежными партнерами также следует руководствоваться положениями «Инструкции по защите коммерческой тайны».

1.3. Инструкция устанавливает режим работы с иностранцами с целью защиты конфиденциальной информации.

1.4. Под работой с иностранцами следует понимать совокупность всех видов деятельности при контактах с иностранными компаниями, фирмами (переписка, телефонные разговоры, передача телексных и факсимильных сообщений) либо личных встреч с их представителями по служебным делам.

1.5. Ответственность за организацию работы с зарубежными партнерами и соблюдение требований настоящей инструкции несут руководство, служба безопасности и руководители соответствующих структурных подразделений фирмы.

1.6. Для работы с зарубежными партнерами ежегодно составляются списки сотрудников, выделенных для этой работы.

2. Основания для работы с зарубежными партнерами

2.1. Основанием для работы с зарубежными партнерами по служебной необходимости являются: планы международных научно-технических связей, заключенные контракты и протоколы, соглашения об установлении прямых производственных, научно-технических связей, ре-

шения о совместной деятельности, а также инициатива самих зарубежных представителей и представителей российской стороны.

2.2. Решение о приеме иностранцев принимается генеральным директором или его заместителями по представлениям руководителей структурных подразделений, согласованных с отделом по международным связям, службой безопасности, техническим отделом и отделом документационного обеспечения.

2.3. Основанием для командирования сотрудников за рубеж служит решение генерального директора или его заместителей, выносимое на основании представляемых руководителями соответствующих отделов материалов, оформленных в установленном порядке. Принятое решение излагается письменно непосредственно на докладной записке, представляемой в установленные сроки.

2.4. В докладной записке отражаются следующие сведения: цель выезда; страна командирования и принимающая организация (фирма); срок командирования; условия финансирования поездки; фамилия, имя, отчество и занимаемая должность командируемого.

3. Прием зарубежных делегаций

3.1. Прием приглашенных зарубежных делегаций

3.1.1. Прием приглашенных зарубежных делегаций осуществляется на основе утвержденных программ, составляемых по установленной форме, а также сметы расходов по приему.

3.1.2. Программы пребывания приглашенных зарубежных делегаций и сметы расходов составляются соответствующими подразделениями, отвечающими за прием, согласовываются с отделом международных связей, службой безопасности и утверждаются генеральным директором.

3.1.3. Ответственным за выполнение программы пребывания иностранной делегации является руководитель соответствующего отдела.

3.2. Организация деловых встреч (переговоров).

3.2.1. Деловые встречи с зарубежными партнерами организуются на основе заявок, оформленных соответствующими отделами, отвечающими за прием по установленной форме.

3.2.2. Заявки согласовываются с руководителем отдела международных связей, службой безопасности, отделом технического обеспечения и утверждаются генеральным директором или его заместителями.

3.2.3. Переводчиков на деловые встречи приглашает отдел, принимающий зарубежных представителей.

3.2.4. Для участия в деловых встречах с зарубежными партнерами, как правило, привлекаются специалисты из числа сотрудников, выделенных для работы с зарубежными представителями, в количестве не менее двух человек.

3.2.5. Деловые встречи могут проводиться в кабинете генерального директора, кабинете его первого заместителя и специально выделенном для этого помещении.

3.2.6. Встречу, сопровождение и проводы зарубежных партнеров осуществляют сотрудники соответствующих отделов и отдела по международным связям.

3.2.7. Лица, участвующие в переговорах, обязаны хранить конфиденциальную информацию фирмы, не входить в обсуждение вопросов, не относящихся к их компетенции.

3.3. Посещение приемов, симпозиумов, семинаров, выставок и других мероприятий, организуемых зарубежными партнерами или с их участием.

3.3.1. Сотрудники фирмы посещают приемы, симпозиумы и семинары, организуемые зарубежными партнерами или с участием зарубежных партнеров, по служебным вопросам по согласованию с отделом международных связей, отделом технического обеспечения и с разрешения генерального директора.

3.3.2. При поступлении письменных или устных приглашений на подобные мероприятия непосредственно в адрес сотрудников следует руководствоваться п. 3.3.1. настоящей инструкции.

3.4. Передача материалов зарубежным представителям.

3.4.1. Передача зарубежным партнерам научно-технических и других материалов допускается после их предварительного рассмотрения руководством и службой безопасности с целью определения возможности их передачи.

4. Ведение служебной переписки

4.1. Общие положения.

4.1.1. Руководство фирмы, отделы и подразделения фирмы ведут служебную переписку, прием и передачу телексных и факсимильных сообщений через отдел документационного обеспечения.

4.1.2. Вся входящая международная корреспонденция (вне зависимости от ее вида) регистрируется и первично рассматривается в отделе документационного обеспечения.

4.1.3. Корреспонденция докладывается генеральному директору или его заместителям, или направляется на рассмотрение и исполнение непосредственно в отделы.

4.1.4. После рассмотрения руководством корреспонденция в соответствии с резолюцией направляется исполнителям, и контроль за сроками исполнения поручения осуществляется в соответствии с установленным порядком.

4.1.5. Право подписи корреспонденции в адрес зарубежных представительств имеют генеральный директор, его заместители и начальники отделов.

4.1.6. Любая корреспонденция в адрес зарубежных представительств подлежит визированию у руководства и в службе безопасности фирмы. Один экземпляр документов остается в отделе документационного обеспечения.

4.2. Работа с письмами.

4.2.1. Служебные письма, адресуемые зарубежным партнерам, пишутся на фирменных бланках с указанием наименования фирмы на английском языке, а также с разрешенными номерами телефонов, факсов и телексов, выделенных для работы с зарубежными представителями.

4.2.2. Ставить какие-либо штампы и печати на таких письмах не разрешается.

4.2.3. Проекты писем в адрес зарубежных партнеров готовятся в отделах фирмы при строгом соблюдении конфиденциальности. Наименование отдела, фамилия и номер телефона исполнителя письма на подлиннике не указываются, а приводятся на копиях.

4.3. Работа с факсимильными сообщениями.

4.3.1. Все факсимильные сообщения от иностранцев подлежат регистрации в отделе документационного обеспечения.

4.3.2. Подготовка проектов факсимильных сообщений осуществляется отделами на бланках, используемых для письменной корреспонденции и со специальным титульным листом. Тексты сообщений могут быть как на русском, так и на иностранных языках.

4.3.3. Передача факсимильных сообщений иностранцам осуществляется отделами со специально выделенного аппарата факсимильной связи с предварительной регистрацией в отделе документационного обеспечения.

4.4. Ведение телефонных разговоров.

4.4.1. Сотрудники фирмы могут вести телефонные разговоры с зарубежными партнерами с телефонов, выделяемых для этих целей в каждом отделе: список телефонов подлежит согласованию с отделом международных связей и службой безопасности.

5. Командирование за рубеж

5.1. Состав делегаций, командируемых за рубеж за счет собственных средств, формируется соответствующими отделами и согласовывается с отделом международных связей, службой безопасности и руководством фирмы.

5.2. При командировании за рубеж по служебной линии делегациям и отдельным специалистам выдается техническое задание, в котором отражается перечень конкретных вопросов, для решения которых организуется поездка.

5.3. Технические задания составляются отделом международных связей и представляются на утверждение руководству не позднее чем за две недели до выезда. Оформление выездных документов производится в отделе международных связей в установленном порядке.

6. Оформление результатов работы с иностранцами, учет и отчетность

6.1. Соответствующие отделы, принимающие иностранцев, по итогам работы с зарубежными партнерами и командирования за рубеж составляют отчеты произвольной формы. По итогам деловых встреч составляются записи бесед по установленной форме.

6.2. Записи бесед представляются в отдел по международным связям в двухдневный срок после окончания работы с иностранцами, а отчеты, как правило, — в двухнедельный срок (два печатных экземпляра).

6.3. В записях бесед и отчетах указывается: когда, где, с кем состоялась встреча; ее основание и цель; кем дано разрешение на встречу, какое учреждение, организацию или фирму представляли иностранцы, их фамилии и должностное положение; кто присутствовал со стороны фирмы; содержание беседы (существо вопросов и ответы на них); какая документация и какие образцы изделий и материалов переданы зарубежным представителям или получены от них, обязательства сторон по существу обсуждавшихся вопросов, а также другая заслуживающая внимания информация.

6.4. Отдел международных связей ведет учет принимаемых иностранных делегаций и деловых встреч, а также учет сообщений от фирмы о контактах с иностранцами.

7. Организационные мероприятия по результатам работы с иностранцами

7.1. Отчеты по результатам работы с зарубежными представительствами и записи бесед, содержание обязательства и предложения сторон докладываются соответствующими отделами, организовавшими встречу, руководству фирмы и службе безопасности.

7.2. Координация работ по выполнению поручений руководства по данным документам возлагается на отдел международных связей и службу безопасности.

7.3. Контроль за выполнением положений настоящей инструкции возлагается на руководство фирмы, отдел международных связей и службу безопасности.

Ответ:

Практическая работа № 22
«Использование критериев подбора сотрудников в подразделения защиты информации»

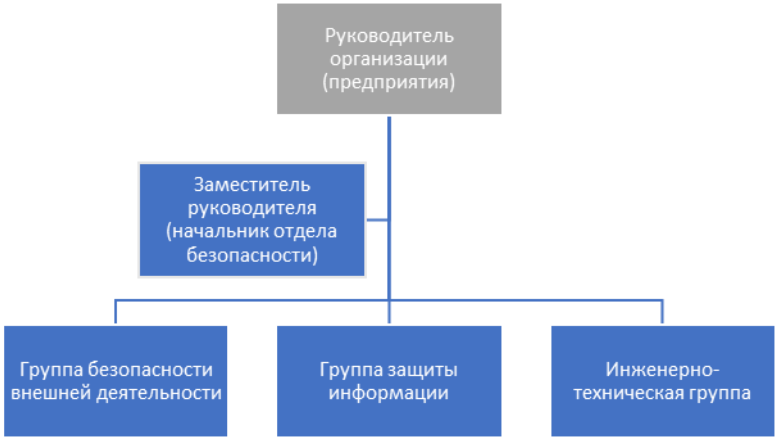
Цель практического занятия: научиться отбирать кандидатов в подразделение защиты информации и составлять критерии для поиска кандидатов

Задание:

По заданным критериям подобрать сотрудников в подразделения защиты информации, учитывая вид деятельности вашей организации

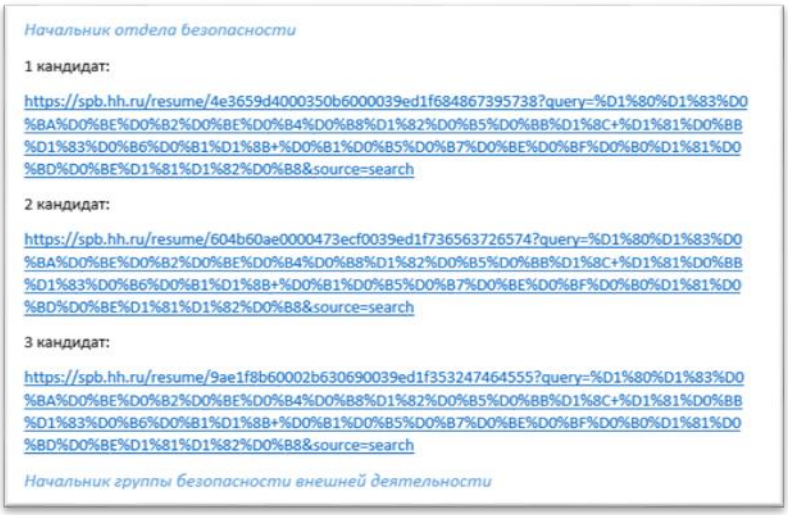
Организация

_____



Пояснение к заданию:

1. Уточнить и дополнить критерии подбора сотрудников в подразделения защиты информации:
   - ✓ Начальник отдела безопасности — руководящая должность, в подчинении которого может быть от 10 человек; начальники групп являются старшими в своей группе сотрудниками, в подчинении могут быть 1-3 человека
   - ✓ Записать кратко какие нормативные документы должны знать будущие сотрудники
   - ✓ Какой необходим опыт работы для претендента на данную должность
   - ✓ Какие знания и опыт будут интересны вам при подборе сотрудников на данную должность в вашу организацию
   - ✓ Кратко записать необходимые умения, которые должны быть у претендента на данную должность в вашу организацию.
   - ✓ Разрешается критерии по возрасту и образованию изменить, дополнив в таком случае своими пояснениями.
2. На каждую должность подобрать по 3 резюме из Интернета (в резюме может иначе называться должность, например, «руководитель отдела безопасности» и т.п.)
   - ✓ Ссылки на резюме сохранить в файл Пр3_МДК0102. Образец оформления задания показан на рисунке.


Начальник отдела безопасности

1 кандидат:

https://spb.hh.ru/resume/4e3659d4000350b6000039ed1f684867395738?query=%D1%80%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D0%B8%D1%82%D0%B5%D0%BB%D1%8C+%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D1%8B+%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8&source=search

2 кандидат:

https://spb.hh.ru/resume/604b60ae0000473ecf0039ed1f736563726574?query=%D1%80%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D0%B8%D1%82%D0%B5%D0%BB%D1%8C+%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D1%8B+%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8&source=search

3 кандидат:

https://spb.hh.ru/resume/9ae1f8b60002b630690039ed1f353247464555?query=%D1%80%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D0%B8%D1%82%D0%B5%D0%BB%D1%8C+%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D1%8B+%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8&source=search

Начальник группы безопасности внешней деятельности

3. После подбора резюме по каждому кандидату написать причины, по которым вы подобрали их.

1. *Начальник отдела безопасности*

🗁 Примерные критерии:

☞ Возраст: старше 40 лет

☞ Образование: высшее

☞ Знание необходимых нормативных документов:

_____

_____

_____

☞ Опыт работы: _____

☞ Знание и опыт работы в сфере деятельности вашей организации_____
_____
☞ Необходимые умения: _____
_____
_____

2. *Начальник группы безопасности внешней деятельности*

🗁 Примерные критерии:

☞ Возраст: старше 30 лет
☞ Образование: высшее
☞ Знание необходимых нормативных документов: _____
_____
_____
☞ Опыт работы: _____
☞ Знание и опыт работы в сфере деятельности вашей организации_____
_____
☞ Необходимые умения: _____
_____
_____

3. *Начальник группы защиты информации*

🗁 Примерные критерии:

☞ Возраст: старше 30 лет
☞ Образование: высшее техническое
☞ Знание необходимых нормативных документов: _____
_____
☞ Опыт работы: _____
☞ Знание и опыт работы в сфере деятельности вашей организации_____
_____
☞ Необходимые умения: _____
_____
_____

4. *Начальник инженерно-технической группы*

🗁 Примерные критерии:

☞ Возраст: старше 30 лет
☞ Образование: высшее техническое
☞ Знание необходимых нормативных документов: _____
_____
☞ Опыт работы: _____
☞ Знание и опыт работы в сфере деятельности вашей организации_____
_____
☞ Необходимые умения: _____
_____
_____

5. *Аналитик по защите информации*

🗁 Примерные критерии:

☞ Возраст: не имеет значения
☞ Образование: высшее техническое
☞ Знание необходимых нормативных документов: _____
_____
☞ Опыт работы: _____
☞ Знание и опыт работы в сфере деятельности вашей организации_____
_____
☞ Необходимые умения: _____
_____
_____

6. *Инженер по защите информации*

🗁 Примерные критерии:

☞ Возраст: не имеет значения
☞ Образование: высшее техническое
☞ Знание необходимых нормативных документов: _____
_____
☞ Опыт работы: _____
☞ Знание и опыт работы в сфере деятельности вашей организации_____
_____
☞ Необходимые умения: _____
_____
_____

7. *Специалист по защите информации*

🗁 Примерные критерии:

☞ Возраст: не имеет значения
☞ Образование: среднее или высшее
☞ Знание необходимых нормативных документов: _____
_____
☞ Опыт работы: _____
☞ Знание и опыт работы в сфере деятельности вашей организации_____
_____
☞ Необходимые умения: _____
_____
_____

8. *Техник по защите информации*

🗁 Примерные критерии:

☞ Возраст: не имеет значения
☞ Образование: среднее
☞ Знание необходимых нормативных документов: _____
_____
☞ Опыт работы: _____
☞ Необходимые умения: _____
_____
_____

Пояснение выбора резюме сотрудников по каждому кандидату:

1. *Начальник отдела безопасности*

1 кандидат: _____
2 кандидат: _____
3 кандидат: _____

2. *Начальник группы безопасности внешней деятельности*

1 кандидат: _____
2 кандидат: _____
3 кандидат: _____

3. *Начальник группы защиты информации*

1 кандидат: _____
2 кандидат: _____
3 кандидат: _____

4. *Начальник инженерно-технической группы*

1 кандидат: _____
2 кандидат: _____

3 кандидат: _____

5. *Аналитик по защите информации*

1 кандидат: _____
2 кандидат: _____
3 кандидат: _____

6. *Инженер по защите информации*

1 кандидат: _____
2 кандидат: _____
3 кандидат: _____

7. *Специалист по защите информации*

1 кандидат: _____
2 кандидат: _____
3 кандидат: _____

8. *Техник по защите информации*

1 кандидат: _____
2 кандидат: _____
3 кандидат: _____

Практическая работа № 23
«Использование критериев подбора сотрудников в подразделения защиты информации»

Цель практического занятия: научиться использовать критерии подбора сотрудников и расставлять в разные подразделения с учётом критериев

Задание:

По заданным критериям расставить сотрудников в подразделения защиты информации вашей организации.

Пояснение к заданию:

- ✓ Сотрудников отбираем и расставляем из подобранных в практической работе № 3.
- ✓ Учитываем запрашиваемую заработную плату.
- ✓ Учитываем опыт работы в данной сфере деятельности.
- ✓ Сотрудников может быть несколько с одной должностью, например, в группу защиты информации.
- ✓ Можно добавить/изменить должности, например, в инженерно-техническую группу, а значит добавить новые резюме.

В таблицу 1 запишите какого кандидата вы выбрали из трёх на должность и почему именно его.

Таблица 1 — Подбор сотрудников в подразделения защиты информации

Должности:	Какого кандидата выбрали? (1/2/3)	Почему выбрали именно этого кандидата из трёх резюме?
Начальник отдела безопасности		
Начальник группы безопасности внешней деятельности		

Должности:	Какого кандидата выбрали? (1/2/3)	Почему выбрали именно этого кандидата из трёх резюме?
Начальник группы защиты информации		
Начальник инженерно-технической группы		
Аналитик по защите информации		
Инженер по защите информации		
Специалист по защите информации		
Техник по защите информации		
Охранник		
Сотрудник бюро пропусков		

В таблицу 2 запишите должности + кандидатов из таблицы 1, распределив их по группам.

Таблица 2 — Расстановка сотрудников подразделения защиты информации

Группа защиты информации	Группа безопасности внешней деятельности	Инженерно-техническая группа

Практическая работа № 24 «Составление должностных инструкций для персонала подразделений защиты информации»

Цель практического занятия: научиться составлять должностные инструкции для персонала из готовых шаблонов

Задание:

Составить должностные инструкции на сотрудников подразделений защиты информации, учитывая вид деятельности вашей организации.

Пояснение к заданию:

- ✓ Создать папку Пр5_0102. В папку поместить должностные инструкции на каждого сотрудника из таблицы. Инструкции назвать по порядковому номеру в таблице.
- ✓ Оформление должностных инструкций привести в соответствие с корпоративным стилем вашей организации.
- ✓ Для каждого сотрудника дополнить должностную инструкцию в соответствии с должностными обязанностями по вашему виду деятельности организации.
- ✓ Внизу в таблице написать какие номера пунктов были вами добавлены/изменены/удалены.

	Сотрудники	***Какие пункты были добавлены/убраны/изменены в должностной инструкции?***
	Начальник отдела безопасности	
	Начальник группы безопасности внешней деятельности	
	Начальник группы защиты информации	
	Начальник инженерно-технической группы	
	Аналитик по защите информации	
	Инженер по защите информации	
	Специалист по защите информации	
	Техник по защите информации	

Практическая работа № 25 «Составление резюме в соответствии с профессиональным стандартом»

Цель практического занятия: научиться писать своё идеальное резюме

Задание:

Составить «идеальное» резюме на себя на должность техника по защите информации

Пояснение к заданию:

1. Открыть должностную инструкцию техника по защите информации, составленную в соответствии с профессиональным стандартом.
2. При составлении резюме необходимо руководствоваться следующим правилами:

- При написании своего резюме руководствоваться профессиональным стандартом.
- Можно найти шаблон резюме в Интернете, можно воспользоваться шаблонами резюме из стандартных шаблонов Word.
- В резюме должно быть указано образование, информация о курсах повышения квалификации, семинарах, конкурсах по профессиональному мастерству.
- В резюме должна быть ваша фотография.
- В резюме написать ваши знания в соответствии с профессиональным стандартом.
- В резюме написать ваши умения в соответствии с профессиональным стандартом.
- В резюме указать дополнительную информацию о вас, которую вы бы хотели сообщить вашему потенциальному работодателю.
- В интернете посмотреть вакансии, подходящие под ваше резюме. В файл скопировать ссылки на эти вакансии (2-3 ссылки).
- В соответствии с найденными вакансиями скорректировать данные в вашем резюме.