МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

по выполнению практических работ
по дисциплине
«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»
для направления подготовки **10.03.01 Информационная безопасность**
направленность (профиль) **Безопасность компьютерных систем**

Пятигорск
2024

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В методических указаниях содержатся материалы, необходимые для самостоятельной подготовки студентов к выполнению практических работ. В описание работ включены цель работы, порядок ее выполнения, рассмотрены теоретические вопросы, связанные с реализацией поставленных задач, приведена необходимая литература.

Методические указания посвящены курсу «Основы информационной безопасности».

Практикум построен на принципе последовательного изучения объекта исследования с развитием и закреплением знаний и навыков работы.

Результаты работы представляются, как правило, в виде файлов, формат и наименование которых определяется требованиями по оформлению.

Каждая работа заканчивается контрольными вопросами, позволяющими провести самоконтроль и укрепить теоретические знания и практические навыки.

Состав и оформление проекта приводится в соответствие с действующими на сегодняшний день нормами и требованиями государственных стандартов РФ.

1. ЦЕЛЬ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование набора общекультурных и профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 Информационная безопасность.

Задачами освоения дисциплины являются: формирование базовых понятий в области информационной безопасности и защиты информации, осознание места и роли информационной безопасности в системе национальной безопасности РФ и выработка первоначальных практических навыков по защите документов на персональном компьютере.

2. ОБОРУДОВАНИЕ И МАТЕРИАЛЫ

Аппаратные средства: персональный компьютер.

Программные средства: ОС MS Windows, MS Office.

Учебный класс оснащен IBM-совместимыми компьютерами, объединенными в локальную сеть. Локальная сеть учебного класса имеет постоянный доступ к сети Internet по выделенной линии. Для проведения лабораторных работ необходимо 10 ПК.

3. УКАЗАНИЯ ПО ТЕХНИКЕ БЕЗОПАСНОСТИ

Перед началом работы следует убедиться в исправности электропроводки, выключателей, штепсельных розеток, при помощи которых оборудование включается в сеть, наличии заземления компьютера, его работоспособности.

Для снижения или предотвращения влияния опасных и вредных факторов необходимо соблюдать санитарные правила и нормы, гигиенические требования к персональным электронно-вычислительным машинам.

Во избежание повреждения изоляции проводов и возникновения коротких замыканий не разрешается: вешать что-либо на провода, закрашивать и белить шнуры и провода, закладывать провода и шнуры за газовые и водопроводные трубы, за батареи отопительной системы, выдергивать штепсельную вилку из розетки за шнур, усилие должно быть приложено к корпусу вилки.

Для исключения поражения электрическим током запрещается: часто включать и выключать компьютер без необходимости, прикасаться к экрану и к тыльной стороне блоков компьютера, работать на средствах вычислительной техники и периферийном оборудовании мокрыми руками, работать на средствах вычислительной техники и периферийном оборудовании, имеющих нарушения целостности корпуса, нарушения изоляции проводов, неисправную индикацию включения питания, с признаками электрического напряжения на

корпусе, класть на средства вычислительной техники и периферийном оборудовании посторонние предметы.

Запрещается под напряжением очищать от пыли и загрязнения электрооборудование.

Во избежание поражения электрическим током, при пользовании электроприборами нельзя касаться одновременно каких-либо трубопроводов, батарей отопления, металлических конструкций, соединенных с землей.

После окончания работы необходимо обесточить все средства вычислительной техники и периферийное оборудование. В случае непрерывного учебного процесса необходимо оставить включенными только необходимое оборудование.

4. СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ РАБОТ

Практическое занятие №1. Оценка рисков информационной безопасности на основе методики OCTAVE

Цель работы: освоить на практике процесс оценки рисков информационной безопасности на основе методики OCTAVE.

Теоретическая часть

На сегодняшний день вопрос оценки рисков информационной безопасности является актуальным для многих предприятий. Информационный риск – это возможность наступления случайного события в информационной системе предприятия, приводящего к нарушению ее функционирования, снижению качества информации, в результате которых наносится ущерб предприятию. Связано это в первую очередь с модернизированной нормативно-правовой базой, позволяющей четко определять наказания и штрафы для операторов систем защиты конфиденциальной информации, не обеспечивающих принципы конфиденциальности, целостности и доступности последней.

Но разберемся, зачем нужно исследовать риски в сфере ИБ и что это может дать при разработке системы обеспечения ИБ для ИС. Для любого проекта, требующего финансовых затрат на его реализацию, весьма желательно уже на начальной стадии определить, что мы будем считать признаком завершения работы и как будем оценивать результаты проекта. Для задач, связанных с обеспечением ИБ это более чем актуально.

На практике наибольшее распространение получили два подхода к обоснованию проекта подсистемы обеспечения безопасности.

Первый из них основан на проверке соответствия уровня защищенности ИС требованиям одного из стандартов в области информационной безопасности. Это может быть *класс* защищенности в соответствии с требованиями руководящих документов ФСТЭК России, *профиль защиты*, разработанный в соответствии со стандартом ISO-15408, или какой-либо другой набор требований. Тогда критерий достижения цели в области безопасности - это выполнение заданного набора требований. *Критерий эффективности* - минимальные суммарные *затраты* на выполнение поставленных функциональных требований:

Вместе с этим сформулированные понятия уровня исходной защищенности и вероятности реализации угрозы не позволяют оператору получить полное представление о защищенности ценных ресурсов и спрогнозировать возможный ущерб при их разглашении, удалении или изменении. Существующие методики оценки рисков информационной безопасности (CRAMM, FRAP, RiskWatch, OCTAVE и др.) позволяют спрогнозировать возможный ущерб.

Наиболее интересной и многосторонней является методика OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation, в переводе с англ. – «оперативная оценка критических угроз, активов и уязвимостей»).

В основе ее работы лежит дерево, имеющее вершины «Ресурс», «Уязвимость», «Угроза», «Ущерб», «Риск». В данной статье предпринята попытка проецирования данной

методики на процесс оценки рисков предприятий разного профиля на территории Российской Федерации. Алгоритм оценки рисков информационной безопасности (ИБ) на предприятии в соответствии с методикой OCTAVE состоит из нескольких этапов (рисунок):

1) Определение активов организации
2) Определение ценности активов организации (S_i).
3) Определение угроз и соответствующих им уязвимости.
4) Оценка вероятности реализации угроз (V_{ry}).
5) Определение риска информационной безопасности (R).
6) Формирование плана по снижению риска ИБ [1].

На рис. 1 представлена блок-схема алгоритма оценки рисков ИБ в соответствии с методикой OCTAVE

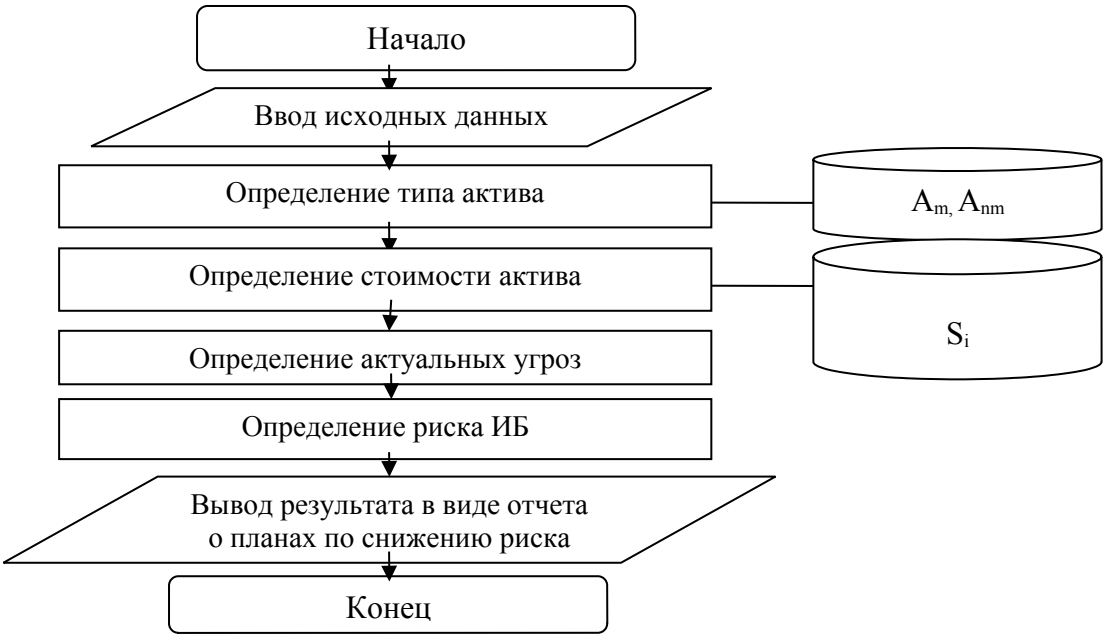


Рис. 1.

Блок-схема алгоритма оценки рисков ИБ в соответствии с методикой OCTAVE

Пример расчета риска для условной организации – ООО «Олимп»:

1) На данном этапе необходимо определить все активы организации. Целесообразно разделить их на материальные (A_m) и нематериальные (A_{nm}) (табл. 1).

Таблица 1.

Определение активов организации

№ п/п	**Материальные активы (A_m)**	**№ п/п**	**Нематериальные активы (A_{nm})**
1.1	Производственное оборудование	2.1	Персональные данные (личные дела сотрудников, медицинские карты)
1.2	Электронно-вычислительные машины	2.2	Коммерческая тайна (бизнес-план, секрет производства)
1.3	Комплектующие изделия	2.3	Иная конфиденциальная информация

2) Для определения ценности активов организации необходимо определить их возможную стоимость или тот денежный ущерб, который может быть нанесен вследствие разглашения, удаления или изменения данного актива.

Для удобства оценки рисков информационной безопасности используем балльную систему. Для оценки стоимости активов введем соответствующие баллы (табл. 2).

Таблица 2. Определение ценности активов организации

№ актива	Основание для оценки актива	Стоимость актива (S_i)	№ актива	Основание для оценки актива	Стоимость актива (S_i)
1.1	Производственное оборудование	10 баллов (≥ 1 000 000 руб.)	2.1	Персональные данные	6 баллов (500 000 т.руб.)
1.2	Электронно-вычислительные машины	2 балла (> 10 000 т.руб.)	2.2	Коммерческая тайна	6 баллов (120 000 т.руб.)
1.3	Комплектующие изделия	6 баллов (> 100 000 т.руб.)	2.3	Иная конфиденциальная информация	2 балла (50 000 т.руб.)

3) На следующем этапе оценки рисков ИБ определяем угрозы безопасности информации и соответствующие им уязвимости (табл. 3) [2].

Таблица 3. Перечень угроз и соответствующих им уязвимостей

№ п/п	Угрозы	Уязвимости
1	Утечка видовой информации	Отсутствие жалюзи на окнах
		Расположение ПК мониторами к окнам
2	Утечка акустической информации	Отсутствие шумогенератора
3	Кража носителей информации	Хранение носителей информации за пределами сейфа
		Отсутствие системы контроля доступа
		Отсутствие системы видеонаблюдения
		Отсутствие системы охранной сигнализации
4	Утечка информации по каналам ПЭМИН	Отсутствие экранирования кабельных коммуникаций
5	Преднамеренное уничтожение информации	Отсутствие утвержденного «Положения о разграничении доступа»
		Отсутствие программной системы разграничения доступа типа Secret Net
		Отсутствие системы контроля доступа, КПП
		Отсутствие утвержденного «Положения о защите конфиденциальной информации, обрабатываемой в организации»
6	Непреднамеренное уничтожение информации	Отсутствие системы резервного копирования
		Отсутствие учета доступа сотрудников к конфиденциальной информации
7	Установка ПО, не связанного с исполнением служебных обязанностей	Отсутствие средств доверенной загрузки
8	Действия вредоносных программ	Не установлено сертифицированное антивирусное ПО
		Отсутствие средств резервного

		копирования
9	Угрозы несанкционированного доступа по каналам связи	Отсутствие средств межсетевого экранирования
10	Стихийное бедствие	Отсутствие противопожарной системы
11	Непреднамеренная модификация (уничтожение) информации сотрудниками	Отсутствие средств защиты от НСД

4) На следующем этапе определяем вероятность реализации угроз - V_{ry}. Предварительно необходимо указать наличие средств защиты в организации (табл. 4).

Таблица 4. Фрагмент опросной таблицы «Оценка вероятности реализации угроз»

№ п/п	**Угроза**	**Средство нейтрализации угрозы**	**Имеется ли на объекте данное средство защиты?**	
			Да	Нет
1	Утечка видовой информации	Жалюзи на окнах	+	
2	Утечка акустической информации	Шумогенератор		+
3	Кража носителей информации	Сейфы для хранения носителей информации	+	
		Система контроля доступа		+
		Система видеонаблюдения	+	
		Охранная сигнализация	+	
4	Утечка информации по каналам ПЭМИН	Экранирование кабельных коммуникаций		+
5	Преднамеренное уничтожение информации	Система видеонаблюдения	+	
		Сигнализация	+	
		Решетки на окнах		+
		КПП		+
6	Непреднамеренное уничтожение информации	Учет доступа сотрудников к конфиденциальной информации		+
		Средства резервного копирования		+
7	Установка ПО, не связанного с исполнением служебных обязанностей	Средства доверенной загрузки	+	
8	Действия вредоносных программ	Антивирусное сертифицированное ПО на ПК сотрудников		+
		Средства резервного копирования		+
9	Угрозы несанкционированного доступа по каналам связи	Средства межсетевого экранирования	+	
10	Стихийное бедствие	Противопожарная система	+	
11	Непреднамеренная модификация (уничтожение) информации сотрудниками	Средства защиты от НСД	+	

19 – 100%
10 – x%
1000/19=53%

Вероятность реализации угроз (V_{ry}) определяется следующим образом:

- V_{ry}=1 - в случае наличия на объекте средств защиты не менее 50 % от общего числа средств защиты;

- V_{ry}=5 - в случае отсутствия на объекте средств защиты от 50 % до 80 % от общего числа средств защиты;

- V_{ry}=10 - в случае отсутствия более 80 % средств защиты.

В приведенном фрагменте опросной таблицы (табл. 4) на объекте необходимо наличие 19 различных средств защиты. Из них отсутствует 57% средств защиты, следовательно, V_{ry}=5.

5) Для определения риска информационной безопасности (R) воспользуемся формулой:

$$R= S_{*}V_{ry}, \qquad (1)$$

где:

V_{ry} – вероятность реализации угрозы;

S – ценность всех активов, определяемое выражением:

$$S_{=}, \qquad (2)$$

где:

S_i – стоимость активов, по которым проводится расчет риска.

Если проводится расчет риска для активов «Электронно-вычислительные машины» и «Коммерческая тайна», то S=2+6=8 (балов), а R=5*8=40.

6) Определив значение риска, мы можем сформировать план по его снижению. Для этого необходимо определить величину риска ИБ, выраженную через качественный показатель (табл. 5) и временное значение риска ИБ по таблице 6 в зависимости от показателя вероятности реализации угроз (V_{ry}).

Таблица 5. Определение величины риска ИБ

	R						
V_{ry}	**60-100**	**50-59**	**30-49**	**20-29**	**10-29**	**6-9**	**2-5**
10	Высокая	Средняя	Средняя	Низкая	Низкая	Низкая	Низкая
5	Высокая	Высокая	Средняя	Средняя	Низкая	Низкая	Низкая
1	Высокая	Высокая	Высокая	Высокая	Высокая	Средняя	Низкая

Для R=40 и V_{ry} = 5 качественный показатель величины риска ИБ будет: Средняя.

Если проводить расчет риска для активов «Производственное оборудование» и/или «Комплектующие изделия», то Перечень угроз и соответствующих им уязвимостей необходимо скорректировать под данные активы.

Определим временное значение риска ИБ по таблице 6 для нашего показателя вероятности реализации угроз (V_{ry}). План по снижению риска: на среднюю перспективу

Таблица 6. Определение временных значений риска ИБ

V_{ry}	**План по снижению риска**

1	Долговременный
5	На среднюю перспективу
10	Списки задач на ближайшее время

На основании данных табл. 5-6 можно сделать вывод о том, что план по снижению риска индивидуален для каждой вероятности реализации угроз.

Иллюстрация процесса оценки риска ИБ по методике OCTAVE на примере условной организации – ООО «Олимп» представлена в табл. 7.

Таблица 7. Процесс оценки риска ИБ

Активы организации	**Ценность актива**	**Вероятность реализации угрозы**	**Риск ИБ**	**Величина риска ИБ**	**План по снижению риска**
ЭВМ+ Коммерческая тайна	S= 8	$V_{гу}$= 5	R=40	Средняя	На среднюю перспективу

В отличие от прочих методик, OCTAVE не предполагает привлечения для исследования безопасности ИС сторонних экспертов, а вся документация по OCTAVE общедоступна и бесплатна, что делает методику особенно привлекательной для предприятий с жестко ограниченным бюджетом, выделяемым на цели обеспечения ИБ.

Таким образом, с помощью использования основ методики OCTAVE можно однозначно определить риск информационной безопасности.

Задания

Для выполнения лабораторной работы необходимо:

1) Описать активы организации согласно примера, представленного в табл. 1. Для этого учесть, что активами организации являются электронно-вычислительные машины и персональные данные.
2) Определить ценности активов организации согласно примера, представленного в табл. 2.
3) Определить угрозы и соответствующих им уязвимости. Для этого взять за основу таблицу 3, при необходимости дополнить её.
4) Определить вероятность реализации угроз - $V_{гу}$ (табл. 4). Для заполнения таблицы использовать варианты заданий, приведенные в таблице 8. Вариант задания определяется по порядковому номеру студента в списке преподавателя.

Таблица 8.

Варианты исходных данных для определения вероятности реализации угроз

№ п/п	**Средство нейтрализации угрозы**	**Варианты с имеющимися на объекте средствами защиты**																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	Жалюзи на окнах	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
2	Шумогенератор		+	+	+	+	+	+	+	+					+	+	+	+	+	+	+
3	Сейфы для хранения носителей информации	+			+	+	+	+	+	+	+	+	+	+				+	+	+	+
	Система контроля доступа				+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
	Система видеонаблюдения					+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

№ п/п	Средство нейтрализации угрозы	Варианты с имеющимися на объекте средствами защиты																		
	Сохранная сигнализация						+	+	+	+	+	+	+	+	+	+	+	+	+	+
4	Экранирование кабельных коммуникаций							+	+	+	+	+	+	+	+	+	+	+	+	+
5	Система видеонаблюдения								+	+	+	+	+	+	+	+	+	+	+	+
	Сигнализация									+	+	+	+	+	+	+	+	+	+	+
	Решетки на окнах										+	+	+	+	+	+	+	+	+	+
	КПП																			
6	Учет доступа сотрудников к конфиденциальной информации												+	+	+	+	+	+	+	+
	Средства резервного копирования																		+	+
7	Средства доверенной загрузки																	+	+	+
8	Антивирусное сертифицированное ПО на ПК сотрудников										+	+	+					+	+	+
	Средства резервного копирования																		+	+
9	Средства межсетевого экранирования																			+
10	Противопожарная система	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
11	Средства защиты от НСД																			+

5) Определить ценность всех активов по формуле (2).
6) Определить риск информационной безопасности по формуле (1).
7) Сформировать план по снижению риска, воспользовавшись таблицами 5-6.
8) Проиллюстрировать процесс оценки риска ИБ, воспользовавшись таблицей 7.
9) Оформить отчёт.
10) Ответить на контрольные вопросы.
11) Сделать вывод.

Контрольные вопросы:

1. Раскройте понятие информационного риска.
2. Перечислите этапы оценки риска по методике OCTAVE.
3. Что подразумевается под критерием эффективности?
4. Назовите способы предотвращения риска.

Список литературы

Перечень основной литературы:

1. Голембиовская, О.М. Оценка рисков безопасности информационных систем персональных данных/О.М. Голембиовская, В.И. Аверченков, М.Ю. Рытов//Информация и безопасность. – Воронеж, 2 12. – №3. – С. 321 – 328.

2. Формализация подходов к обеспечению защиты персональных данных, обрабатываемых в информационных системах: монография/ О.М.Голембиовская, М.Ю.Рытов, К.Е.Шинаков. – Брянск: БГТУ, 2014. – 189 с.

Перечень дополнительной литературы:

1 Булгакова С.В. Управленческий учет : учебник для бакалавров / С.В. Булгакова ; Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Воронежский государственный университет», Министерство образования и науки РФ. - Воронеж : Издательский дом ВГУ, 2015. - 370 с. - Библиогр.: с. 357-364. - ISBN 978-5-9273-2193-3 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=441585.

2. Гринберг, А.С. Документационное обеспечение управления: учебник / А.С. Гринберг, Н.Н. Горбачёв, О.А. Мухаметшина. - Москва : Юнити-Дана, 2015. - 391 с. : табл., граф., ил., схемы - Библиогр.: с. 382-383. - ISBN 978-5-238-01770-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=115031.

Интернет-ресурсы:

1. Университетская библиотека online. http://www.biblioclub.ru.
2. ЭБС «IPRbooks». http://www.iprbookshop.ru.
3. Электронная библиотека СКФУ.. http://catalog.ncstu.ru.
4. Государственная публичная научно- техническая библиотека России. (ГПНТБ России). www.gpntb.ru.

Практическое занятие №2. Разработка политики информационной безопасности предприятия: верхний уровень

Цель работы: изучить существующие стандарты международного и отечественного уровня в области построения политики безопасности.

Актуальность темы

Актуальность разработки политик информационной безопасности для компаний объясняется необходимостью создания механизма управления и планирования информационной безопасности. Также политики ИБ позволяют совершенствовать следующие направления деятельности компании: поддержка непрерывности бизнеса; повышение уровня доверия к компании; привлечение инвестиций и т.д. Естественно, что совершенствование направлений деятельности организации зависит от грамотности составления политики информационной безопасности.

Теоретическая часть

Для организаций общий подход и намерения в области обеспечения информационной безопасности (ОИБ), официально выраженные руководством, отражаются в разработанном, утвержденном им и строго выполняемом на практике всеми ее сотрудниками и бизнес-партнерами документе – Политика ИБ организации.

Политика ИБ непосредственно связана с законодательством в области ОИБ. Она представляет собой директиву и выражает позицию высшего руководства организации по отношению к деятельности в области ОИБ за счет создания программы ОИБ, установки ее целей и распределения обязанностей, а также стремление организации соответствовать государственным, международным требованиям и стандартам в этой области. Таким образом.

Политика ИБ организации является основой для разработки целого ряда документов в области ОИБ: стандартов, руководств, процедур, практик, регламентов, должностных инструкций и пр.

Политика ИБ организации определяется как:

- совокупность требований и правил по ОИБ для объекта ИБ, выработанных в соответствии с требованиями руководящих и нормативных документов в целях противодействия заданному множеству угроз ИБ, с учетом ценности защищаемой информационной сферы и стоимости системы ОИБ (СОИБ);
- документированные решения в области ОИБ;
- совокупность (одно или несколько) документированных правил, процедур, практических приемов в области безопасности, которыми руководствуется организация в своей деятельности;
- документацию, определяющую высокоуровневые цели, содержание и основные направления и устанавливающую правила, процедуры, практические приемы и руководящие принципы ОИБ активов организации, которыми она руководствуется в своей деятельности.

Политика информационной безопасности представляет собой комплекс документов, отражающих все основные требования к обеспечению защиты информации и направления работы предприятия в этой сфере. При построении политики безопасности можно условно выделить три ее основных уровня: верхний, средний и нижний.

Верхний уровень политики информационной безопасности предприятия служит:

- для формулирования и демонстрации отношения руководства предприятия к вопросам информационной безопасности и отражения общих целей всего предприятия в этой области;

- основой для разработки индивидуальных политик безопасности (на более низких уровнях), правил и инструкций, регулирующих отдельные вопросы;
- средством информирования персонала предприятия об основных задачах и приоритетах предприятия в сфере информационной безопасности.

Примерная схема представлена на рисунке 1.

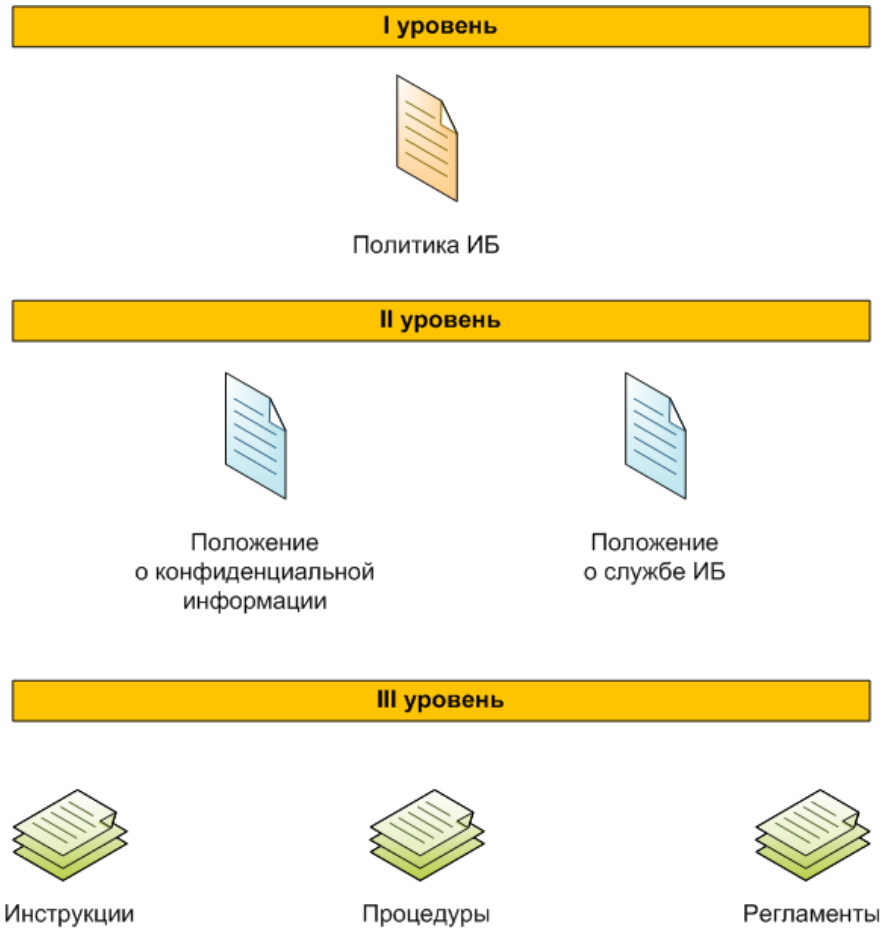


Рисунок 1. Структура нормативно-методических документов в области ИБ

При разработке политик безопасности всех уровней необходимо придерживаться следующих основных правил:

- Политики безопасности на более низких уровнях должны полностью подчиняться соответствующей политике верхнего уровня, а также действующему законодательству и требованиям государственных органов.
- Текст политики безопасности должен содержать только четкие и однозначные формулировки, не допускающие двойного толкования.
- Текст политики безопасности должен быть доступен для понимания тех сотрудников, которым он адресован.

В целом политика информационной безопасности должна давать ясное представление о требуемом поведении пользователей, администраторов и других специалистов при внедрении и использовании информационных систем и средств защиты информации, а также при осуществлении информационного обмена и выполнении операций по обработке информации. Кроме того, из политики безопасности, если она относится к определенной технологии и/или методологии защиты информации, должны быть понятны основные принципы работы этой технологии. Важной функцией политики безопасности является четкое разграничение ответственностей в процедурах информационного обмена: все заинтересованные лица должны ясно осознавать границы как своей ответственности, так и

ответственности других участников соответствующих процедур и процессов. Также одной из задач политики безопасности является защита не только информации и информационных систем, но и защита самих пользователей (сотрудников предприятия и его клиентов и контрагентов).

Политика информационной безопасности на этом уровне может определять и описывать:

- собственно, решение об осуществлении целенаправленной систематической деятельности по обеспечению информационной безопасности предприятия;
- перечень основных информационных ресурсов, таких как информационные системы, массивы данных, информация об отдельных фактах и явлениях (конструкторских разработках, коммерческих сделках, результатах НИОКР и т.п.), защита которых имеет наибольший приоритет для всего предприятия;
- общий подход к распределению ответственности за обеспечение информационной безопасности внутри организации;
- указание на необходимость для всего персонала соблюдать определенные меры предосторожности при работе с информацией и информационными системами, повышать свою квалификацию в данной области и осознавать меру ответственности за возможные нарушения;
- отношение руководства предприятия к фактам нарушения требований по обеспечению информационной безопасности и лицам, совершающим такие нарушения, а также общий подход к их преследованию в случае выявления таких фактов.

Задания

На лабораторном занятии необходимо:

1) дать описание организации политики информационной безопасности для конкретного предприятия, закреплённого за каждым студентом согласно порядковому номеру в списке преподавателя (см. приложение Б).

Отчет раздела политики ИБ «1. Общие положения» должен включать следующие главы:

1. Назначение политики информационной безопасности.
2. Основные принципы обеспечения ИБ.
3. Соответствие ПБ действующему законодательству.
4. Ответственность за реализацию политик информационной безопасности.
5. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе.
6. Защищаемые информационные ресурсы Организации.

Для описания раздела политики ИБ «1. Общие положения» конкретного предприятия использовать характеристики организаций, приложение Б и шаблон политики ИБ, приложение В.

2) Оформить отчёт.
3) Ответить на контрольные вопросы.
4) Сделать вывод.

Контрольные вопросы:

1. Кто утверждает все оформленные решения, формирующие ПБ?
2. Кто несёт ответственность обеспечения защиты информации?
3. Перечислите категории информационных ресурсов, подлежащих защите в Организации.
4. Кто несёт ответственность за сохранность персональных данных сотрудника организации?

Список литературы

Перечень основной литературы:

1 Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс]/ Анисимов А.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 212 с.— Режим доступа: http://www.iprbookshop.ru/52182.— ЭБС «IPRbooks», по паролю.

2. Бирюков А.Н. Процессы управления информационными технологиями [Электронный ресурс]/ Бирюков А.Н.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 263 с.— Режим доступа: http://www.iprbookshop.ru/52165.— ЭБС «IPRbooks», по паролю.

Перечень дополнительной литературы:

1 Булгакова, С.В. Управленческий учет : учебник для бакалавров / С.В. Булгакова ; Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Воронежский государственный университет», Министерство образования и науки РФ. - Воронеж : Издательский дом ВГУ, 2015. - 370 с. - Библиогр.: с. 357-364. - ISBN 978-5-9273-2193-3 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=441585.

2. Гринберг, А.С. Документационное обеспечение управления: учебник / А.С. Гринберг, Н.Н. Горбачёв, О.А. Мухаметшина. - Москва : Юнити-Дана, 2015. - 391 с. : табл., граф., ил., схемы - Библиогр.: с. 382-383. - ISBN 978-5-238-01770-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=115031.

Интернет-ресурсы:

1. Университетская библиотека online. http://www.biblioclub.ru.
2. ЭБС «IPRbooks». http://www.iprbookshop.ru.
3. Государственная публичная научно- техническая библиотека России. (ГПНТБ России). www.gpntb.ru.

Практическое занятие №3. Разработка политики информационной безопасности предприятия: средний уровень

.

Цель работы: изучить существующие стандарты международного и отечественного уровня в области построения политики безопасности.

Актуальность темы

Актуальность разработки политик информационной безопасности для компаний объясняется необходимостью создания механизма управления и планирования информационной безопасности. Также политики ИБ позволяют совершенствовать следующие направления деятельности компании: поддержка непрерывности бизнеса; повышение уровня доверия к компании; привлечение инвестиций и т.д. Естественно, что совершенствование направлений деятельности организации зависит от грамотности составления частных политик информационной безопасности.

Теоретическая часть

Средний уровень документов по обеспечению ИБ составляют документы, определяющие правила, требования и принципы, используемые применительно к отдельным областям ИБ, видам и технологиям деятельности организации.

Кроме того, в состав документов данного уровня рекомендуется включить планы работ по обеспечению ИБ организации и стандарты технологий обеспечения ИБ организации.

Политики информационной безопасности среднего уровня определяют отношение предприятия (руководства предприятия) к определенным аспектам его деятельности и функционирования информационных систем:

- отношение и требования (более детально по сравнению с политикой верхнего уровня) предприятия к отдельным информационным потокам и информационным системам, обслуживающим различные сферы деятельности, степень их важности и конфиденциальности, а также требования к надежности (например, в отношении финансовой информации, а также информационных систем и персонала, которые относятся к ней);
- отношение и требования к определенным информационным и телекоммуникационным технологиям, методам и подходам к обработке информации и построения информационных систем;
- отношение и требования к сотрудникам предприятия как к участникам процессов обработки информации, от которых напрямую зависит эффективность многих процессов и защищенность информационных ресурсов, а также основные направления и методы воздействия на персонал с целью повышения информационной безопасности.

В планах работ по обеспечению ИБ рекомендуется описывать перечень, порядок, объем (в той или иной форме), сроки выполнения мероприятий по реализации задач обеспечения ИБ организации, а также указывать руководителей, исполнителей и ответственность за выполнение этих мероприятий.

К разработке и согласованию политик обеспечения ИБ второго уровня рекомендуется привлекать представителей:

- руководства организации и профильных подразделений;
- служб информатизации и безопасности.

Документы среднего уровня могут быть утверждены руководителем организации, его заместителем по вопросам ИБ или иными должностными лицами, в компетенцию которых входят вопросы, отраженные в этих документах.

Задания

Для выполнения лабораторной работы необходимо:

1) Описать частные политики, содержащие принципы и рекомендации по отдельным аспектам информационной безопасности.
2) Оформить отчёт.
3) Ответить на контрольные вопросы.
4) Сделать вывод.

Варианты частных политик ИБ приведены в таблице 2.

Таблица 2.

Пример состава политик ИБ

№ п/п	Политики ИБ	Стандарты
1	Политика управления рисками	BS ISO/IEC 27005:2011
2	Политика безопасность персонала	ГОСТ Р ИСО/МЭК 27001-2006
3	Политика физической безопасности	ГОСТ Р ИСО/МЭК 27001-2006
4	Политика допустимого использования информационных ресурсов	ГОСТ Р ИСО/МЭК 27001-2006
5	Политика использование мобильных устройств	ГОСТ Р ИСО/МЭК 27001-2006
6	Политика защиты от вредоносного ПО	ГОСТ Р ИСО/МЭК 27001-2006

7	Политика управления установкой (инсталяцией) компонентов программного обеспечения	ГОСТ Р ИСО/МЭК 27001-2006
8	Политика обеспечения доверенной загрузки средств вычислительно техники	ГОСТ Р ИСО/МЭК 27001-2006
9	Политика использования криптографического контроля	ГОСТ Р ИСО/МЭК 27001-2006
10	Политика резервного копирования	ГОСТ Р ИСО/МЭК 27001-2006
11	Политика контроля состава технических средств, программного обеспечения и средств защиты информации	ГОСТ Р ИСО/МЭК 27001-2006
12	Политика дистанционной работы	Письмо ФСТЭК России от 20 марта 2020 г. N 240/84/389
13	Политика использования сетевых служб	ГОСТ Р ИСО/МЭК 27001-2006
14	Политика по работе с инцидентами информационной безопасности	ГОСТ Р ИСО/МЭК ТО 18044-2007
15	Политика обеспечения непрерывности ИТ-сервисов	ГОСТ Р 53647.1-2009
16	Политика обеспечения восстановления	Р 50.1.095—2014
17	Предоставление услуг сторонним организациям	ГОСТ Р ИСО/МЭК 27001-2006

Для описания частной политики информационной безопасности конкретного предприятия использовать шаблоны 1-17, приложение Г.

Контрольные вопросы:

1. Кем могут быть утверждены документы второго уровня?
2. Какие документы составляют средний уровень документов по обеспечению ИБ?
3. Какие положения определяют планы по обеспечению ИБ?
4. Кого рекомендуется привлекать к разработке и согласованию политик обеспечения ИБ второго уровня?

Список литературы

Перечень основной литературы:

1 Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс]/ Анисимов А.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 212 c.— Режим доступа: http://www.iprbookshop.ru/52182.— ЭБС «IPRbooks», по паролю.

2. Бирюков А.Н. Процессы управления информационными технологиями [Электронный ресурс]/ Бирюков А.Н.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 263 c.— Режим доступа: http://www.iprbookshop.ru/52165.— ЭБС «IPRbooks», по паролю.

Перечень дополнительной литературы:

1 Булгакова, С.В. Управленческий учет : учебник для бакалавров / С.В. Булгакова ; Федеральное государственное бюджетное образовательное учреждение высшего

профессионального образования «Воронежский государственный университет», Министерство образования и науки РФ. - Воронеж : Издательский дом ВГУ, 2015. - 370 с. - Библиогр.: с. 357-364. - ISBN 978-5-9273-2193-3 ; То же [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=441585.
2. Гринберг, А.С. Документационное обеспечение управления: учебник / А.С. Гринберг, Н.Н. Горбачёв, О.А. Мухаметшина. - Москва : Юнити-Дана, 2015. - 391 с. : табл., граф., ил., схемы - Библиогр.: с. 382-383. - ISBN 978-5-238-01770-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=115031.

Интернет-ресурсы:

1. Университетская библиотека online. http://www.biblioclub.ru.
2. ЭБС «IPRbooks». http://www.iprbookshop.ru.
3. Государственная публичная научно- техническая библиотека России. (ГПНТБ России). www.gpntb.ru.

Практическое занятие №4. Определение класса автоматизированной системы

Цель работы: освоить методику определения класса АС.

1. Теоретическая часть

Данное задание предполагает использование документа «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.»

Классификации подлежат автоматизированные системы, для которых необходима защита конфиденциальной информации от несанкционированного доступа.

Деление АС на соответствующие классы производится с учётом условий их функционирования. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- режим обработки данных в АС - коллективный или индивидуальный.

Устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в
зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно

обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

2. Методика и порядок выполнения работы.

На данном занятии студенты:
- изучают документ «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.»;
- определяют класс АС по данному РД, п. 1.9;
- оформляют акт классификации, смотри приложение Е.

3. Задание.

Для объекта защиты по варианту, назначенного преподавателем (по порядковому номеру студента в списке), студенты определяют класс автоматизированной системы. Содержание исходных данных дано в таблице 1.

Таблица 1.

Исходные данные для выполнения работы

№ варианта	**Защищаемые информационные ресурсы**	**Уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;**	**Режим обработки данных в АС**
1.	Персональные данные	одинаковые права доступа (полномочия) ко всей информации АС	коллективный
2.	Конфиденциальная информация	одинаковые права доступа (полномочия) ко всей информации АС	индивидуальный
3.	Персональные данные	не все пользователи имеют право доступа ко всей информации АС	коллективный
4.	Конфиденциальная информация	одинаковые права доступа (полномочия) ко всей информации АС	индивидуальный
5.	Персональные данные	одинаковые права доступа (полномочия) ко всей информации АС	коллективный
6.	Конфиденциальная информация	не все пользователи имеют право доступа ко всей информации АС	коллективный
7.	Персональные данные	одинаковые права доступа (полномочия) ко всей информации АС	индивидуальный

8.	Конфиденциальная информация	одинаковые права доступа (полномочия) ко всей информации АС	коллективный
9.	Персональные данные	не все пользователи имеют право доступа ко всей информации АС	коллективный
10.	Конфиденциальная информация	одинаковые права доступа (полномочия) ко всей информации АС	индивидуальный
11.	Персональные данные	одинаковые права доступа (полномочия) ко всей информации АС	коллективный
12.	Конфиденциальная информация	не все пользователи имеют право доступа ко всей информации АС	коллективный
13.	Персональные данные	одинаковые права доступа (полномочия) ко всей информации АС	индивидуальный
14.	Конфиденциальная информация	одинаковые права доступа (полномочия) ко всей информации АС	коллективный
15.	Персональные данные	не все пользователи имеют право доступа ко всей информации АС	коллективный
16.	Конфиденциальная информация	одинаковые права доступа (полномочия) ко всей информации АС	индивидуальный
17.	Персональные данные	одинаковые права доступа (полномочия) ко всей информации АС	коллективный
18.	Конфиденциальная информация	одинаковые права доступа (полномочия) ко всей информации АС	индивидуальный
19.	Персональные данные	не все пользователи имеют право доступа ко всей информации АС	коллективный
20.	Конфиденциальная информация	одинаковые права доступа (полномочия) ко всей информации АС	индивидуальный

Наименование АС для Акта классификации взять из приложения Б.

4. Содержание отчёта и его форма

Отчет по лабораторной работе оформляется в программной оболочке Microsoft Word (других редакторах) и предоставляется преподавателю в электронном виде с расширением «.doc».

Отчет по лабораторной работе должен состоять из следующих структурных элементов:
- титульный лист (см. Приложение А);
- вводная часть;
- основная часть (описание работы):
    - ответы на вопросы;
    - заключения и выводы.
- Приложение: акт классификации.

Зашита отчета по лабораторной работе заключается в предъявлении преподавателю полученных результатов в виде файла и демонстрации полученных навыков при ответах на вопросы преподавателя.

5. Контрольные вопросы

1. Перечислите классы автоматизированных систем.
2. Перечислите группы автоматизированных систем.
3. Какие АС считаются многопользовательскими?
4. Что понимается под уровнем конфиденциальности информации?

Практическое занятие №5. Определение требований по защите информации от НСД для АС

Цель работы: научится формировать требования по защите информации от несанкционированного доступа для конкретного класса АС.

1. Теоретическая часть

Данное задание предполагает использование документа «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.»

Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД определяются в зависимости от класса АС в рамках этих подсистем должны быть реализованы требования.

2. Методика и порядок выполнения работы.

На данном занятии студенты:
- изучают документ «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.»;
- для своего класса АС, определенного на практическом занятии 5, формируют перечень требований по защите информации в соответствии с содержанием РД, пп. 2.4, 2.7 и 2.10;
- оформляют перечень требований по защите информации в АС с использованием

нумерации.

3. Задание.

Определить перечень требований по защите информации в АС для своего класса АС.

4. Содержание отчёта и его форма

Отчет по лабораторной работе оформляется в программной оболочке Microsoft Word (других редакторах) и предоставляется преподавателю в электронном виде с расширением «.doc».

Отчет по лабораторной работе должен состоять из следующих структурных элементов:

- титульный лист (см. Приложение А);
- вводная часть;
- основная часть (описание работы):
- заключения и выводы.

Зашита отчета по лабораторной работе заключается в предъявлении преподавателю полученных результатов в виде файла и демонстрации полученных навыков при ответах на вопросы преподавателя.

5. Контрольные вопросы

1. Что понимается под термином идентификация?
2. Что представляет собой аутентификация?
3. Что понимается под шифрованием информации?
4. Каково назначение подсистемы обеспечения целостности?

Практическое занятие №6. Правила формирования паролей

Цель работы: научиться формировать пароли пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.

1. Теоретическая часть

Для выполнения мероприятия идентификация и аутентификация субъектов доступа и объектов доступа потребуется устанавливать пароли и настраивать локальные политики безопасности компьютера в отношении паролей.

Данная процедура позволит избежать случайного удаления, или просто доступа к конфиденциальной информации. Помимо длины пароля, также необходимо установить максимальное время жизни пароля, и требование от пользователей ввода сложных паролей, что также добавит определенной защищенности от взлома учетных записей.

Пароль - это строка знаков, применяемая для доступа к информации или компьютеру. Парольные фразы обычно длиннее паролей и содержат несколько слов, образующих отдельную фразу, что обеспечивает дополнительную безопасность. Применение паролей и парольных фраз позволяет предотвратить несанкционированный доступ пользователей к файлам, программам и другим ресурсам. Рекомендуется создавать надежные пароли и парольные фразы, которые сложно раскрыть или взломать. Рекомендуется применять надежные пароли для всех учетных записей пользователей на компьютере. При использовании рабочей сети администратор сети может установить обязательное

использование надежных паролей.

Примечание: в беспроводной сети дополнительную безопасность парольной фразы обеспечивает применение ключа безопасности WPA. Такая парольная фраза преобразуется в ключ, используемый для шифрования и не отображаемый пользователю.

Таблица 1.

Признаки надежных паролей и парольных фраз

Надежный пароль:	**Надежная парольная фраза:**
• Состоит как минимум из восьми знаков. • Не содержит имени пользователя, действительного имени или названия компании. • Не содержит полного слова. • Значительно отличается от паролей, использовавшихся ранее.	• Имеет длину от 20 до 30 знаков. • Представляет собой последовательность слов, образующих фразу. • Не содержит общих фраз, встречающихся в литературе или музыкальных произведениях. • Не содержит слов, встречающихся в словарях. • Не содержит имени пользователя, действительного имени или названия компании. • Значительно отличается от паролей и парольных фраз, использовавшихся ранее.

Надежные пароли и парольные фразы содержат знаки, принадлежащие каждой из следующих категорий как показано в таблице 2.

Таблица 2. Примеры знаков, принадлежащих категориям

Категория знаков	**Примеры**
Буквы верхнего регистра	A, B, C...
Буквы нижнего регистра	a, b, c ...
Цифры	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Другие знаки на клавиатуре (все знаки, не являющиеся буквами или цифрами) и пробелы	` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /

Пароль или парольная фраза, отвечающие всем описанным выше условиям, по-прежнему могут быть ненадежными. Например, Hello2U! удовлетворяет всем требованиям к надежности, но является ненадежным, так как содержит полное слово. H3ll0 2 U! надежнее предыдущего, так как некоторые буквы в слове замещены цифрами, и, кроме того, пароль содержит пробелы.

Если все же требуется записать пароль или парольную фразу, чтобы не забыть их, убедитесь, что они хранятся в надежном месте и не отмечены фразами вида «мой пароль».

Создание надежных паролей и парольных фраз с использованием знаков ASCII. Для создания паролей и парольных фраз также можно использовать расширенный набор знаков ASCII. Используя расширенный набор знаков ASCII, можно повысить надежность паролей и парольных фраз, так как увеличивается выбор знаков для их создания. Перед использованием знаков из расширенного набора ASCII для создания паролей и парольных фраз следует убедиться, что пароли и фразы с такими знаками совместимы с приложениями, используемыми вами или организацией. Будьте особенно осторожны при использовании знаков из расширенного набора ASCII в паролях и парольных фразах, если в организации используется несколько различных операционных систем или версий ОС Windows.

Расширенный набор знаков ASCII находится в таблице символов. Некоторые знаки из расширенного набора ASCII не следует использовать в паролях. Не используйте знак, если для него не указана комбинация клавиш в нижнем правом углу диалогового окна «Таблица символов». Дополнительные сведения см. в разделе Использование специальных символов (таблица символов): вопросы и ответы.

Пароли Windows могут содержать гораздо больше восьми символов,

рекомендованных ранее. Допускается создание паролей длиной до 127 знаков.

2. Методика и порядок выполнения работы.

Чтобы научиться создавать надёжную запоминающуюся парольную фразу, следуйте приведенным ниже рекомендациям.

1. Создайте сокращение из легко запоминаемой фразы. Например, фразы, значимой для вас, такой как: мой сын родился 12 декабря 2004 года.
2. Замещайте цифрами, знаками, а также орфографическими ошибками буквы или слова в легко запоминающейся фразе. Например, на основе фразы мой сын родился 12 декабря 2004 года можно составить надежную парольную фразу м0й $ыН р0д№лс’ 12124. Пароли и парольные фразы могут быть связаны с любимым видом спорта или хобби. Например, Мне нравится играть в бадминтон можно переделать в МнЄНрА8№tся№грAt'вБадDм№нт()н.

Чтобы проверить стойкость своего пароля, необходимо воспользоваться онлайн сервисом: https://password.kaspersky.com/ru/moon-3/ . В диалоговом окне необходимо в ручном режиме ввести созданную парольную фразу.

Чтобы научиться создавать надёжную запоминающуюся парольную фразу в автоматическом режиме с помощью генератора паролей, необходимо воспользоваться сервисом «ИнфоТеКС»: https://infotecs.ru/product/vipnet-password-generator.html#soft. Для скачивания программы ViPNet Password Generator версии 4.1 необходимо заполнить форму (ФИО и e-mail, на который придет ссылка для скачивания файла). Чтобы сгенерировать пароль нужно задать свойства парольной фразы:

- сложность пароля: сложный;
- язык: русский;
- т.д. как показано на рис. 1.

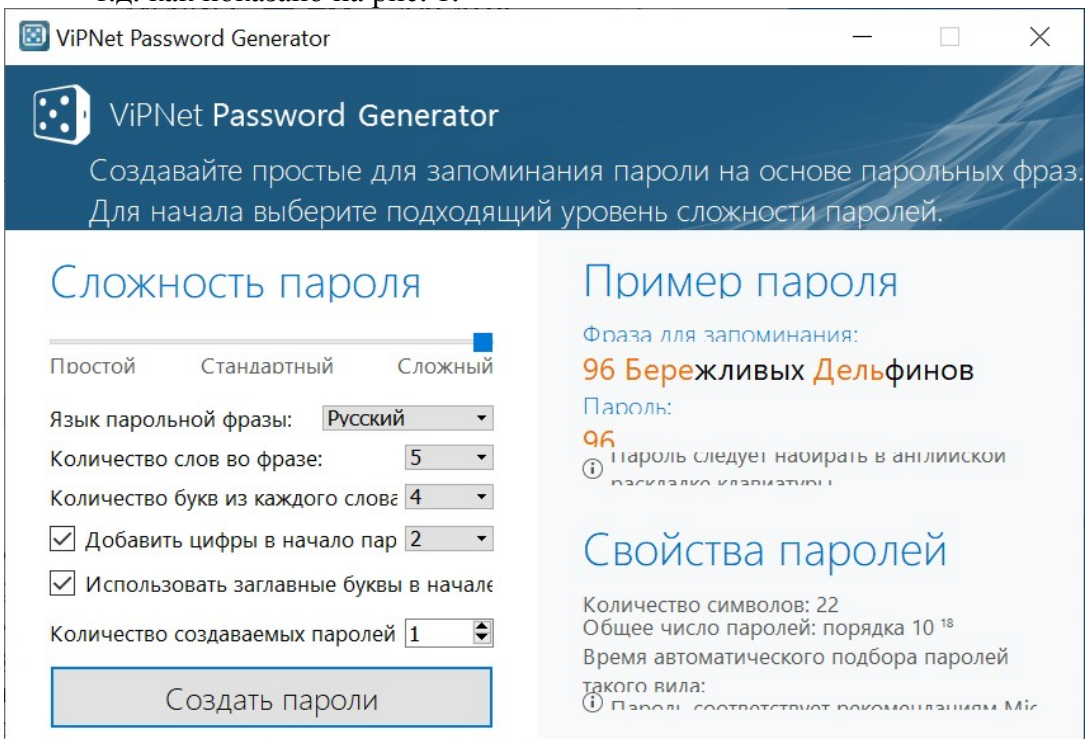


Рисунок 1: Настройка надежности пароля

С помощью программы ViPNet Password Generator возможно одновременно формировать большое число паролей.

3. Задание.

1. Придумайте парольную фразу длиной от 20 до 30 знаков.

2. Сделайте её надёжной, используя следующие категории знаков: буквы верхнего регистра, буквы нижнего регистра, цифры, другие знаки на клавиатуре (все знаки, не являющиеся буквами или цифрами) и пробелы.
3. Проверить стойкость своего пароля, воспользовавшись онлайн сервисом Password.kaspersky.
4. Создать вторую парольную фразу, используя сервис «ИнфоТеКС».
5. Проверить стойкость сгенерированного пароля, воспользовавшись онлайн сервисом Password.kaspersky.
6. Сравнить способ ручного формирования пароля с онлайн-генератором по следующим критериям: простота, удобство запоминания, стойкость, время формирования.

4. Содержание отчета и его форма:

Отчет по лабораторной работе оформляется в программной оболочке Microsoft Word (других редакторах) и предоставляется преподавателю в электронном виде с расширением «.doc».

Отчет по лабораторной работе должен состоять из следующих структурных элементов:

- титульный лист;
- вводная часть;
- основная часть (описание работы):
- заключения и выводы.

Зашита отчета по лабораторной работе заключается в предъявлении преподавателю полученных результатов в виде файла и демонстрации полученных навыков при ответах на вопросы преподавателя.

5. Контрольные вопросы

1. Что представляет собой пароль?
2. Что представляет собой парольная фраза?
3. Как сделать парольную фразу надёжной?
4. Какова должна быть минимальная длина пароля?

Практическое занятие №7. Защита баз данных на примере MS ACCESS с помощью пароля

Цель работы: Изучение способов защиты информации в БД на примере СУБД MS Access с помощью пароля.

1. Основы теории

Основными объектами базы данных Access, которые хранятся в одном файле с расширением .accdb, являются:

- таблицы, запросы, схема данных, которые непосредственно имеют отношение к БД;
- отчеты, формы, модули и макросы, которые называются объектами приложения.

Особенности объектов БД Access **Отчеты и формы** предназначаются для типовых процессов обработки данных, таких как просмотр, обновление, поиск согласно заданным критериям, получение отчетов. Данные объекты приложений строятся из графических элементов, которые называют **элементами управления**. Основные элементы управления предназначены для отображения полей таблиц, которые являются источниками данных объекта. Чтобы автоматизировать доступ к объектам и обеспечить их взаимодействие,

используется программный код. С его помощью получают полноценное пользовательское приложение, доступ к функциям которого обеспечивается с помощью меню, формы и панелей инструментов. Чтобы создать программный код используют макросы и модули на языке VBA.

Таблицы создает пользователь с целью хранения данных, касающихся одной сущности – одного информационного объекта модели данных нужной предметной области. Таблица состоит из записей (строк) и полей (столбцов). В каждом поле содержится одна характеристика информационного объекта рассматриваемой предметной области. Запись содержит сведения об одном экземпляре информационного объекта.

Запросы на изменение предоставляют возможность обновления, удаления или добавления данных в таблицы, а также создания новых таблиц на основе существующих. Схема данных определяет, с помощью каких полей связываются таблицы между собой, каким образом будет происходить выполнение объединения данных рассматриваемых таблиц, необходимо ли выполнять проверку связной целостности при изменении ключей таблиц, удалении и добавлении записей. Формы представляют собой основное средство создания диалогового интерфейса пользовательского приложения.

Форму можно создавать для работы с электронными документами, которые сохраняются в таблицах БД. Форму используют с целью разработки интерфейса для управления приложением. В форму можно включать процедуры обработки событий, которые позволяют управлять обработкой данных в приложении. Подобные процедуры сохраняются в модуле формы. На формы можно добавлять видео, звуковые фрагменты, диаграммы, рисунки. Можно разрабатывать формы с набором вкладок, с помощью которых можно выполнять ту или иную функцию приложения.

Владельцем называется учетная запись пользователя, имеющего контроль над базой данных или ее объектом. По умолчанию владельцем объекта или базы данных является пользователь, создавший их (то есть пользователь, зарегистрированный при открытии базы данных). Учетная запись группы не может быть владельцем базы данных, но может быть владельцем ее объекта. В этом случае все пользователи данной группы являются владельцами этого объекта. Владелец объекта или базы данных обладает исключительными правами, которых его нельзя лишить. Даже если ему не предоставлены определенные права доступа, он может их вернуть, изменив права доступа к объекту или базе данных для себя и других пользователей. Владелец базы данных всегда может открыть ее.

Система безопасности БД должна обеспечивать физическую целостность БД и защиту от несанкционированного вторжения с целью чтения содержимого и изменения данных.

Защита БД производится на двух уровнях:

- на уровне пароля;

-на уровне пользователя (защита учетных записей пользователей и идентифицированных объектов).

Чтобы предотвратить несанкционированное использование базы данных Access, ее можно зашифровать с помощью пароля. После этого расшифровать базу данных и удалить пароль можно будет, только введя его. В этой работе описано, как зашифровать базу данных с помощью пароля, а также расшифровать ее и удалить из нее пароль.

В более ранних версиях Access вы можете создать учетные записи пользователей и пароли с помощью функции безопасности на уровне пользователя. Зашифрованную базу данных, пароль от которой утерян, невозможно использовать. Если пароль неизвестен, его нельзя удалить. Функция шифрования действует только в отношении баз данных в формате ACCDB.

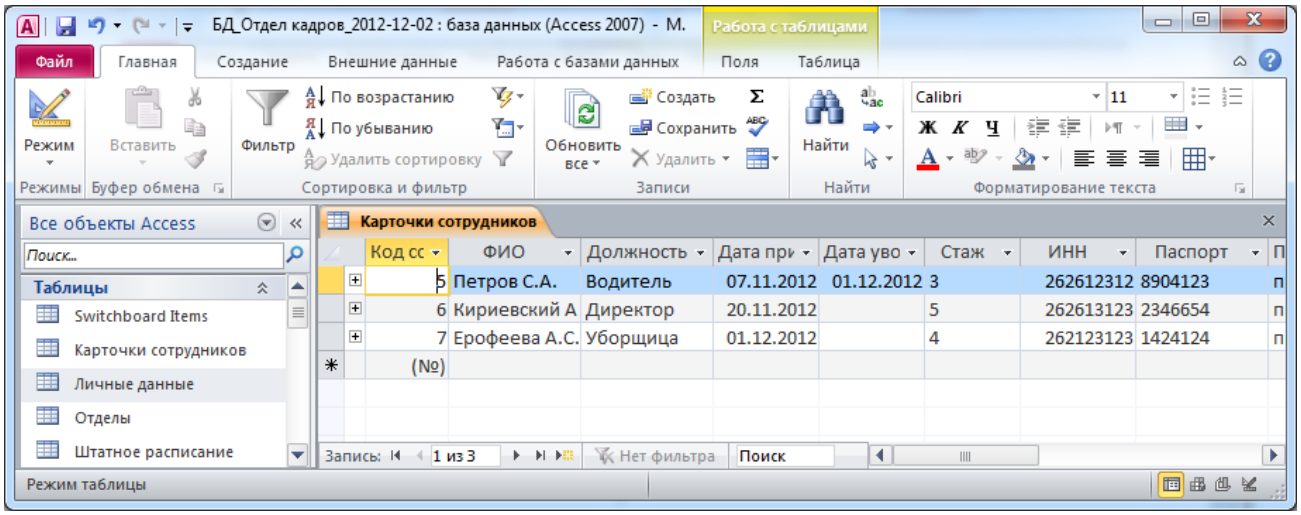
2. Задание к работе

- Создать новую базу данных MS Access.
- Зашифровать базу данных паролем.
- Расшифровать базу данных.

3. Порядок выполнения работы

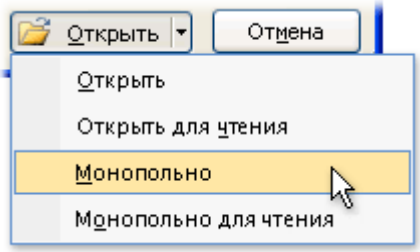
В Access 2010 не поддерживается защита на уровне пользователя для баз данных, созданных в новом формате (ACCDB и ACCDE-файлы). Однако при открытии базы данных из более ранней версии Access, имеющей защиту на уровне пользователя, в Access 2010 эти параметры будут продолжать действовать. Поэтому рассмотрим алгоритм защиты на уровне пароля.

1. Открываем СУБД MS Access и создаем новую базу данных MS Access.

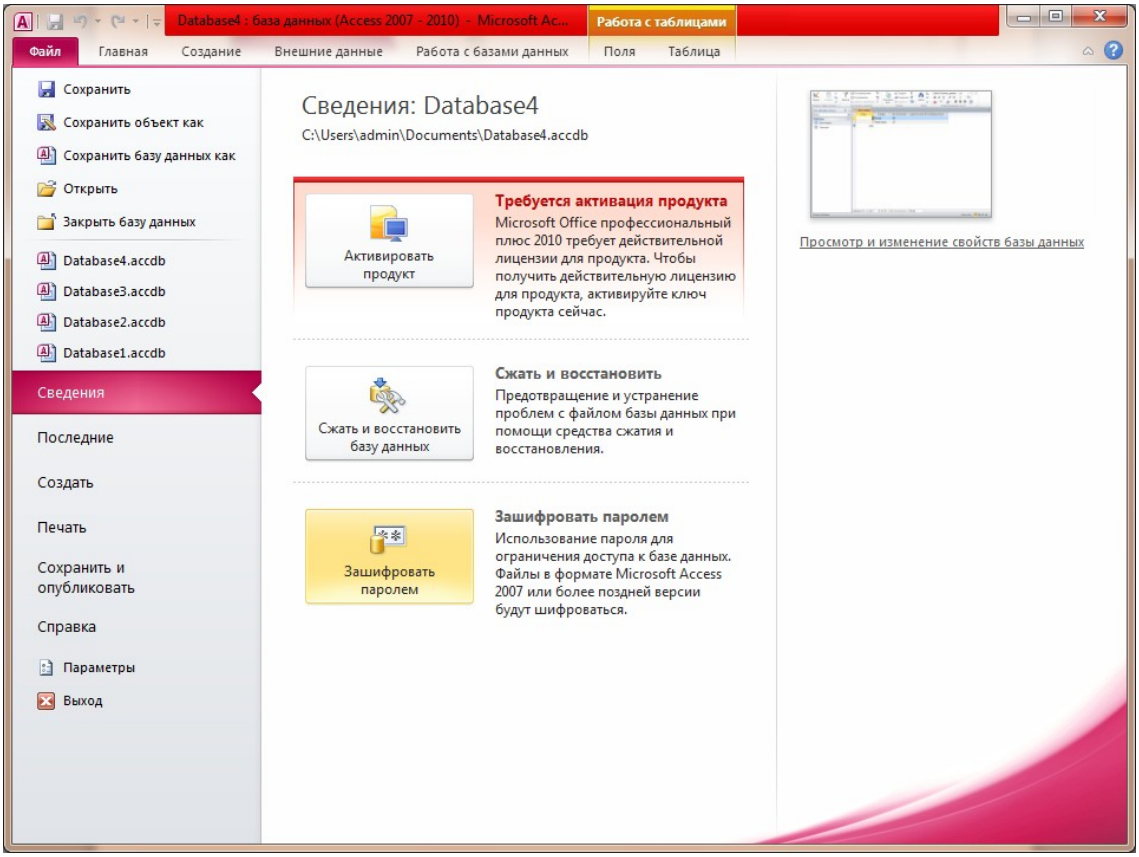


Для формирования базы данных «Персональный учет работников» используется табличная система управления базами данных Microsoft Access. Внутренняя «начинка» базы данных для ведения персонального учета работников в нашем примере будет состоять из следующих таблиц: «Карточки сотрудников», «Личные данные» и т.д. Наиболее часто создаются таблицы в режиме конструктора, т.к. вряд ли найдется такая заготовка у Мастера таблиц, которая подошла бы для решения конкретной, уникальной задачи. Нажимаем кнопку «Создать» на вкладке таблицы и выбираем пункт списка «Конструктор». При создании таблицы определяется ее структура и свойства, при этом получается пустая незаполненная таблица. Строится такая таблица в два этапа: на первом этапе задаются имена полей (столбцов), типы данных каждого поля, свойства полей, первичный ключ таблицы, имя таблицы при сохранении и т.д.; на втором этапе осуществляется ввод данных в макет таблицы.

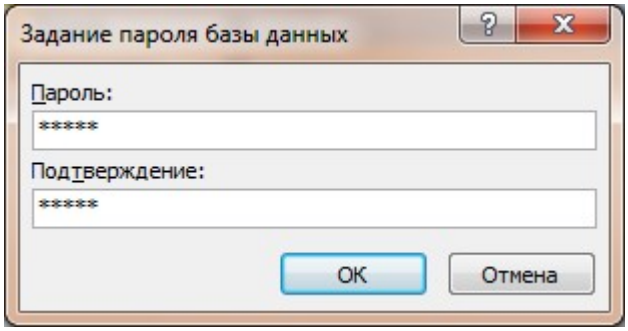
2. Сохраняем созданную БД и закрываем эту БД.
3. Вновь открываем БД, но уже в монопольном режиме.
4. На вкладке Файл нажмите кнопку Открыть.
5. В диалоговом окне Открыть найдите файл, который нужно открыть, и выделите его.
6. Щелкните стрелку рядом с кнопкой Открыть и выберите команду Монопольно.



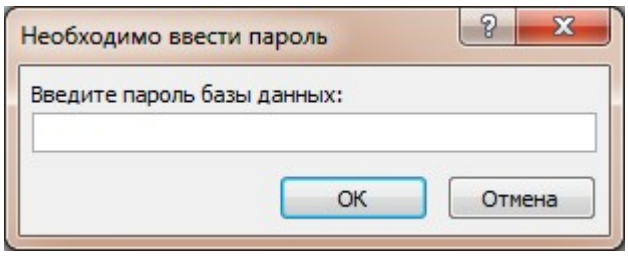
7. На вкладке Файл нажмите кнопку Сведения и выберите пункт Зашифровать паролем.



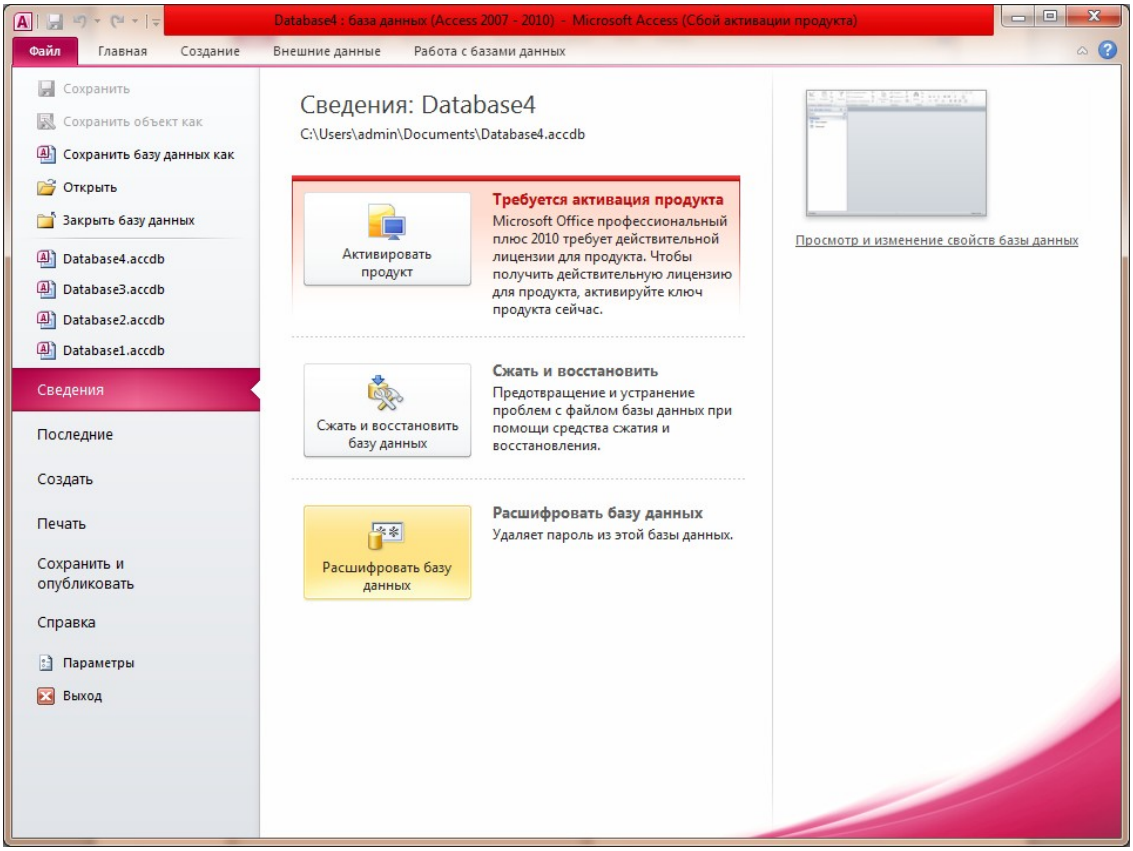
Откроется диалоговое окно Задание пароля базы данных. Введите пароль в поле Пароль, а затем повторите его в поле Проверить.



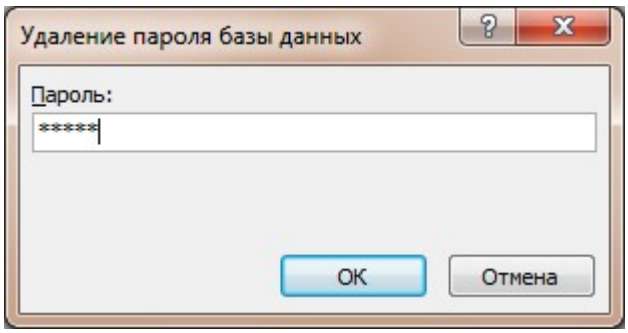
8. Закрыть БД.
9. Открыть защищенную паролем БД в монопольном режиме. Появиться окно «Необходимо ввести пароль». Придумать и ввести пароль.



10. Для удаления созданного пароля необходимо зайти во вкладке Файл нажать кнопку Сведения и выбрать пункт Расшифровать базу данных.



Появится окно Удаления пароля баз данных.



4. Содержание отчета:

Отчет по лабораторной работе оформляется в программной оболочке Microsoft Word (других редакторах) и предоставляется преподавателю в электронном виде с расширением «.doc».

Отчет по лабораторной работе должен состоять из следующих структурных элементов:

- титульный лист (см. Приложение А);
- вводная часть;
- основная часть (описание работы):
- скриншоты о проделанной работе;
- заключения и выводы.

Зашита отчета по лабораторной работе заключается в предъявлении преподавателю полученных результатов в виде файла и демонстрации полученных навыков при ответах на вопросы преподавателя.

5. Контрольные вопросы

1. Способы защиты информации в БД Access.
2. Перечислите объекты БД Access.
3. Раскройте понятие Владельца объекта БД Access.
4. Алгоритм защиты БД Access на уровне пароля.

Практическое занятие №8. Утечка речевой информации. Определение звукоизоляции ограждающих конструкций

Цель: научиться проводить предварительную оценку защищенности выделенных помещений от утечки по акустическому каналу методом формантной разборчивости.

1. Теория

Под акустической информацией обычно понимается информация, носителями которой являются акустические сигналы. В том случае, если источником информации является человеческая речь, **акустическая информация** называется **речевой**. Первичными источниками акустических сигналов являются механические колебательные системы, например органы речи человека, а вторичными - преобразователи различного типа, например, громкоговорители.

В акустических измерениях в качестве измеряемой величины наиболее часто используется звуковое давление *L*. Звуковое давление - это избыточное давление, возникающее в упругой среде при прохождении через нее звуковой волны. Если в качестве упругой среды рассматривать воздушную среду, то звуковое давление - это среднеквадратическое отклонение давления относительно атмосферного давления (рис.1.).

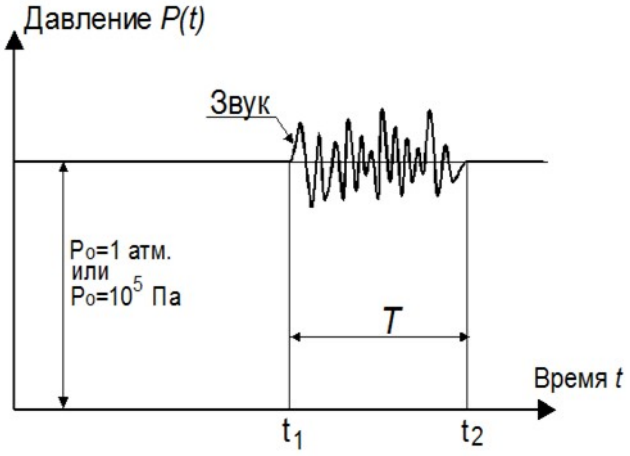


Рис.1. Изменение давление в воздушной среде при возникновении звука

Для обсуждения информации ограниченного доступа (совещаний, обсуждений, конференций, переговоров и т.п.) используются специальные помещения (служебные кабинеты, актовые залы, конференц-залы и т.д.), которые называются ***защищаемыми помещениями (ЗП)***.

Методика оценки утечки речевой информации за пределы границ контролируемой зоны

Для того, чтобы сделать вывод о возможности утечки речевой информации за пределы защищаемого помещения, необходимо провести ряд расчетов по этапам:

1-й этап:

1) определить звукоизоляцию ограждающих конструкций ЗП;

2-й этап:

2) оценить уровень шумов;
3) определить уровень акустического сигнала перед ограждающей конструкцией и за ограждающей конструкцией;

3-й этап:

4) определить понятность и разборчивость речи;
5) оценить результат.

Данная работа предусматривает выполнение расчетов по 1-му этапу.

Звукоизоляция ограждающих конструкций

При падении звуковых волн с интенсивностью $I_{пад}$ на какую-либо перегородку больших размеров в сравнении с длиной волны интенсивность звука с другой стороны перегородки $I_{пр}$ в условиях отсутствия отражения звука в пространстве за перегородкой будет определяться только звукопроводностью перегородки. Коэффициент звукопроводности:

$$\alpha_{пр} = I_{пр} / I_{пад}$$

или в логарифмических единицах (звукоизоляция перегородки — снижение уровня сигнала, проникающего в помещения извне):

$Q_{пер} = L_{пад} - L_{пр}$:, откуда:

$$L_{пр} = L_{пад} - Q_{пер} \qquad (1)$$

где:

$L_{пад}$ – уровень звукового давления с внутренней стороны перегородки;

$L_{пр}$ - уровень звукового давления с внешней стороны перегородки.

Расчет звукоизоляции по значению поверхностной плотности производится по формуле:

$$Qпер(\text{дБ}) = 20 lg\, \rho,$$

где ρ — поверхностная плотность, кг/м^2, отношение массы образца определенного размера к его площади.

Примечание: Поверхностную плотность определяют по ГОСТ Р 50277. [ГОСТ Р 53225 2008].

Коэффициент звукоизоляции стен $Q_{пер}$ с различной поверхностной плотностью ρ в децибелах (с учетом только мембранного переноса) для частот 500...1000 Гц может быть определен по формулам:

2) $Qпер(\text{дБ}) = 12.5 lg\, \rho + 14$ – для стен с ρ <200 кг/ (2)

3) $Qпер(\text{дБ}) = 14.5 lg\, \rho + 15$ – для стен с ρ>200 кг/ (3)

4) $Qпер(\text{дБ}) = 14.3 lg(\rho_1 + \rho_2) + 20 lg - 13$ (4)

Для двойных жестких перегородок с воздушной прослойкой между ними; с поверхностной плотностью $\rho = 30...100 \quad \text{кг/м}^2$,

где:

ρ_1 и ρ_2 - поверхностная плотность первой и второй перегородок,

δ - толщина воздушного слоя между ними.

Расчёт звукоизоляции производится, если отсутствуют рассчитанные значения коэффициентов звукоизоляции, приведенные в табл. 1.

Случай использования неоднородной перегородки.

В качестве неоднородной ограждающей конструкции рассматриваются случаи:

- стена с окном/окнами;
- стена с дверью/дверями.

Учитываются такие параметры, как отношение в процентах площади окна/двери к площади ограждающей конструкции, в которой расположено окно/дверь, величина звукоизоляции глухой части перегородки (стена без учета окна или двери) и величина звукоизоляции двери или окна.

Звукоизолирующая способность определяется из выражения:

$$Q_{пер} = Q_1 - 10\lg\left[1 + \frac{S_0}{S_1 + S_0}\left(10^{0,1(Q_1 - Q_0)} - 1\right)\right] \quad (5)$$

где:

Q_1 — величина звукоизоляции глухой части перегородки (стена без учета окна или двери);

Q_0 — величина звукоизоляции двери или окна;

S_1 — площадь глухой части стены;

S_0 — площадь двери или окна.

Значения коэффициентов звукоизоляции, рассчитанные для некоторых материалов и ограждающих конструкций приведены в табл. 1.

Таблица 1. Значения коэффициентов звукоизоляции материалов и ограждающих конструкций

Материал или конструкция	Толщина, мм	Поверхностная плотность, кг/м2	$Q_{пер}$, дБ
Стены и перегородки:			
Стена из кирпичной кладки без штукатурки (из красного кирпича):			
в 0,5 кирпича	120,0	204,0	48,0
в 1 кирпич	250,0	425,0	53,0
в 1,5 кирпича	380,0	646,0	56,0
в 2 кирпича	520,0	884,0	58,0
в 2,5 кирпича	640,0	1088,0	59,0
Стена из пустотелого кирпича	380,0	-	51,0
Стена из пустотелого кирпича	510,0	-	54,0
Стена из железобетона	100,0	240,0	49,0
Стена из железобетона	140,0	340,0	51,0
Стена из железобетона	160,0	400,0	52,0
Стена из железобетона	180,0	430,0	53,0
Стена из железобетона	200,0	500,0	54,0
Стена из железобетона	300,0	750,0	56,6
Стена из железобетона	800,0	2000,0	62,8
Гипсобетонная (гипсолитовая) плита	80,0	115,0	39,7
Гипсобетонная (гипсолитовая) плита	95,0	135,0	40,6
Газобетонная плита	240,0	270,0	50,25
Керамзитобетонная плита	80,0	100,0	39,0

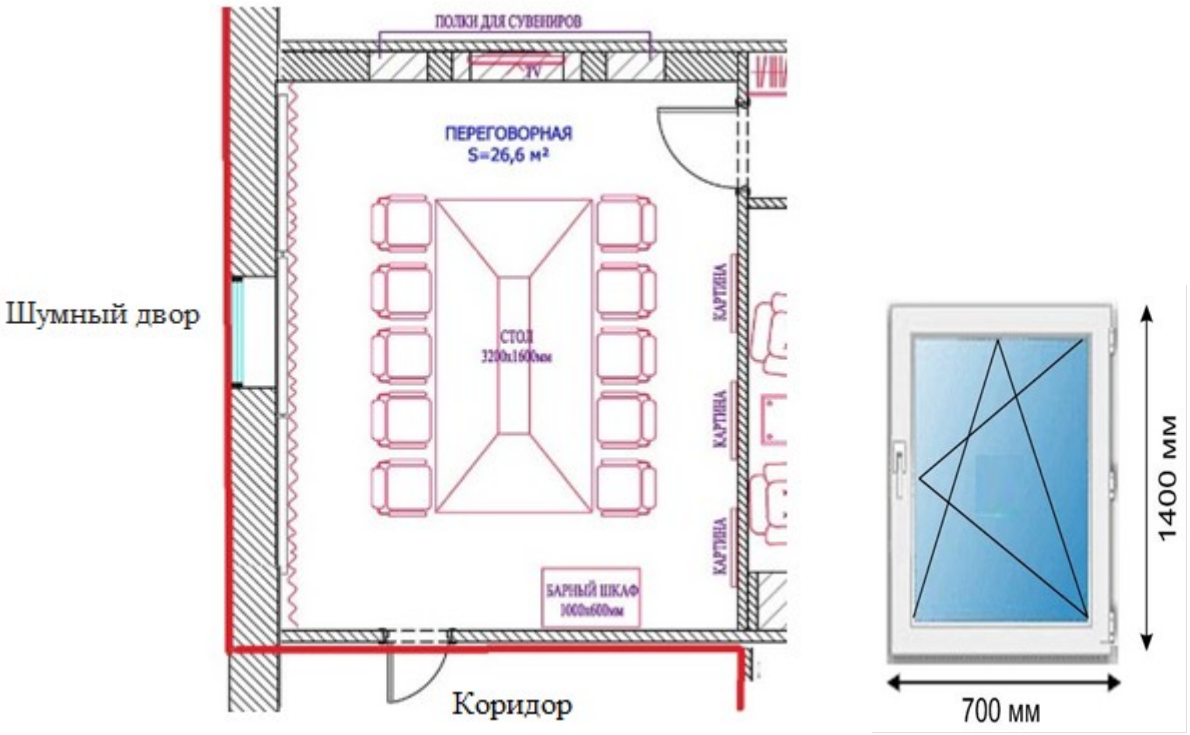
Керамзитобетонная плита	100,0	150,0	41,2
Керамзитобетонная плита	120,0	195,0	42,6
Шлакоблоки, отштукатуренные с двух сторон	220,0	360,0	52,0
Стена из пемзобетона	140,0	150,0	42,0
Стена из пемзобетона	230,0	250,0	50,0
Стена из шлакобетона	140,0	150,0	42,0
Стена из шлакобетона	250,0	400,0	52,7
Стена из шлакобетона из пустотелых пемзобетонных блоков	190,0	190,0	43,0
Стена из шлакобетона из пустотелых пемзобетонных блоков	290,0	270,0	50,0
Перегородка одинарная из досок толщиной 2 см, оштукатуренная с обеих сторон и оклеенная обоями	60,0	70,0	37,0
Перегородка одинарная из досок толщиной 2,5 см, оштукатуренная с обеих сторон по войлоку	70,0	76,0	39,0
Перегородка двойная из брусков 10 см, обшитых с двух сторон досками толщиной 2,5 см и оштукатуренная с двух сторон	180,0	95,0	45,0
Гипсовые пустотелые камни толщиной 1 см с двумя стенками толщиной по 1,5 см и промежутком 8 см с засыпкой шлаком	110,0	117,0	41,0
Перекрытия:			
Несущие железобетонные плиты с круглыми пустотами с конструкцией пола: - паркетная клепка - цементная песчаная наливная стяжка - пергамин в один слой	220,0	376,0	52,3
Несущие железобетонные плиты с круглыми пустотами с конструкцией пола: паркетные доски лаги ленточные прокладки из изоляционных ДВП	220,0	290,0	54,0
Окна:			
Одинарное остекление без уплотнительных прокладок	3,0	-	22,0
Одинарное остекление без уплотнительных прокладок	4,0	-	26,0
Одинарное остекление без уплотнительных прокладок	6,0	-	26,0
Двойное остекление, расстояние между стеклами 57 мм, без звукопоглощающего материала (нар./внутр.)	3,0/3,0	-	32,0

Двойное остекление, расстояние между стеклами 57 мм, со звукопоглощающим материалом (нар./внутр.)	3,0/3,0	-	42,0
Двойное остекление, расстояние между стеклами 90 мм, без звукопоглощающего материала	3,0/3,0	-	38,0
Двойное остекление, расстояние между стеклами 90 мм, со звукопоглощающим материалом	3,0/3,0	-	43,0
Двойное остекление, расстояние между стеклами 57 мм, без звукопоглощающего материала	4,0/4,0	-	38,0
Двойное остекление, расстояние между стеклами 57 мм, со звукопоглощающим материалом	4,0/4,0	-	41,0
Двойное остекление, расстояние между стеклами 90 мм, без звукопоглощающего материала	4,0/4,0	-	41,0
Двойное остекление, расстояние между стеклами 57 мм, без звукопоглощающего материала	6,0/3,0	-	35,0
Двойное остекление, расстояние между стеклами 90 мм, без звукопоглощающего материала	6,0/3,0	-	37,0
Двойное остекление, расстояние между стеклами 38 мм, без звукопоглощающего материала	6,0/6,0	-	40,0
Двойное остекление, расстояние между стеклами 190 мм, без звукопоглощающего материала	6,0/6,0	-	45,0
Двойное остекление, расстояние между стеклами 400 мм, без звукопоглощающего материала	6,0/6,0	-	48,0
Двери:			
Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 4,5 см:			
без уплотняющих прокладок	-	-	18,0
с уплотняющими прокладками	-	-	23,0
Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 2,5 см из 3 мм фанеры без уплотняющих прокладок	-	-	10,0
То же, оклеенная фанерой размером 90х200 см без уплотняющих прокладок	-	-	22,0
Глухая щитовая дверь, толщиной 40 мм, облицованная с двух сторон фанерой, толщиной 4 мм:			
Без уплотняющих прокладок	-	-	24,0
С уплотняющими прокладками	-	-	32,0
Щитовая дверь из твердых древесноволокнистых плит толщиной 4-6 мм с воздушным зазором 50 мм, заполненным стекловатой:			
Без уплотняющих прокладок	-	-	30,0
С уплотняющими прокладками	-	-	33,0
Щитовая дверь из твердых древесноволокнистых			

плит толщиной 4-6 мм с воздушным зазором 50 мм, заполненным минеральный войлоком:			
Без уплотняющих прокладок	-	-	28,0
С уплотняющими прокладками	-	-	32,0
Тяжелая дубовая дверь размером 90х210 см, плотно пригнанная	-	-	25,0
Металлическая дверь (герметичная)	-	-	30,0

Пример расчёта

Рассмотрим возможность утечки речевых сообщений из исследуемого кабинета.



Размеры: 4х5м, h=3м.

Размер двери: 2х0,9м.

Граница контролируемой зоны показана красным. Окно выходит в шумный двор. Дверь выходит в коридор. В исследуемом кабинете имеется:

- одно окно с двойным остеклением и расстоянием между стёклами 57 мм без звукопоглощающего материала с толщиной стекла 3 мм и коэффициентом звукоизоляции Q_{per} = 32 дБ (табл. 1);
- площадь окна составляет 20% от площади всей железобетонной панели толщиной 300 мм и коэффициентом звукоизоляции Q_{per}=56,6 дБ (табл. 1), окно выходит в шумный двор;
- дверь с филенкой из 2,5 см сосновых досок (с двумя панелями) с обвязкой толщиной 4,5 см без уплотняющих прокладок с коэффициентом звукоизоляции Q_{per}=18 дБ (табл. 1);
- площадь двери составляет 16,7% от площади всей гипсолитовой плиты толщиной 80 мм и коэффициентом звукоизоляции Q_{per}=39,7 дБ (табл. 1), дверь выходит в коридор.

Так как в нашем случай использования неоднородной перегородки, то определяем $Q_{пер}$(дБ) по формуле (5).

Подставив соответствующие значения, получим:

- для стены с окном Q_{per}=39 дБ;
- для стены с дверью Q_{per}=25,7 дБ.

Полученные значения звукоизоляций будем использовать при определении уровня акустического сигнала за ограждающей конструкцией.

2. Задание

1) Для помещения, назначенного преподавателем (см. варианты заданий, приложение Ж), определить величины звукоизоляций конструкций на границах контролируемой зоны (отмечены красным).
2) Для формирования исходных данных необходимо выбрать свой вариант объекта защиты согласно порядкового номера в списке преподавателя.

3. Содержание отчета:

Отчет по лабораторной работе оформляется в программной оболочке Microsoft Word (других редакторах) и предоставляется преподавателю в электронном виде с расширением «.doc».

Отчет по лабораторной работе должен состоять из следующих структурных элементов:

- титульный лист (см. Приложение А);
- вводная часть (описание методики);
- основная часть (расчеты);
- вывод.

Зашита отчета по лабораторной работе заключается в предъявлении преподавателю полученных результатов в виде файла и демонстрации полученных навыков при ответах на вопросы преподавателя.

5. Контрольные вопросы

1. Какие помещения называются защищаемыми помещениями?
2. Дайте определение звукового давления.
3. Каков физический смысл звукоизоляции?
4. Как влияет коэффициент звукоизоляции стен *Qпер* на утечку информации по звуковому каналу?

Литература

1. Кученков Е. Б., Музалев Е. А. Экспериментальная оценка акустической защищенности исследуемых помещений // Вопросы защиты информации. - М.: 1999., № 3.
2. Снижение шума в зданиях и жилых районах / Под ред. Осипова Г. Л., Юдина Е.Я. - М: Стройиздат, 1987.
3. Справочник проектировщика. Защита от шума / Под ред. Юдина Е. Я. - М.: Стройиздат, 1974.
4. СНИП 23-03-2003. Защита от шума.
5. Волобуев, С. Защита конфиденциальной речевой информации: простейшие методики / С. Волобуев // Системы безопасности. 2003. - №6(54).

Практическое занятие №9. Утечка речевой информации. Определение уровня шумов и акустических сигналов

Цель: научиться проводить предварительную оценку защищенности выделенных помещений от утечки по акустическому каналу методом формантной разборчивости.

Методика оценки утечки речевой информации за пределы границ контролируемой зоны

Для того, чтобы сделать вывод о возможности утечки речевой информации за пределы защищаемого помещения, необходимо провести ряд расчетов по этапам:

1-й этап:

1) определить звукоизоляцию ограждающих конструкций ЗП;

2-й этап:

2) оценить уровень шумов;
3) определить уровень акустического сигнала перед ограждающей конструкцией и за ограждающей конструкцией;

3-й этап:

4) определить понятность и разборчивость речи;
5) оценить результат.

Данная работа предусматривает выполнение расчетов по 2-му этапу.

Определение уровня акустического сигнала перед ограждающей конструкцией

Для расчетов применяются измеренные значения уровней интенсивности речи, представленные в табл. 2.

Таблица 2. Измеренные уровни звуков

Источник звука	**Уровень интенсивности речи, дБ (f=1000Гц)**
Обычный	55-60
Громкий	65-70
Громкий разговор по телефону	55
Шумное собрание	65-70
Речь с устройства звукоусиления	70-80

Определение уровня акустического сигнала за ограждающей конструкцией

При прохождении через различные строительные конструкции и материалы сигналы ослабевают в зависимости от толщины и поверхностной плотности материала. Уровень акустического сигнала за ограждающей конструкцией (звукоизолирующей перегородкой) $L_{пр}$ м определяется из выражения (1). Предполагая, что в качестве приёмника речевых сообщений используется техническое средство, которое может иметь на низких частотах подъём усиления на 6 дБ, выражение для определения $L_{пр}$ примет следующий вид:

$$L_{пр} = L_{пад} + 6 - Q_{пер} \quad (1)$$

Результат расчета уровня акустического сигнала за ограждающей конструкцией будем использовать для расчёта уровня ощущения формант $E_ф$.

Влияние шумов на восприятие речи

Восприятие речи в значительной степени зависит от уровня акустических шумов, которые вызываются многочисленными источниками - как внешними, находящимися за пределами помещения, так и внутренними. Обычно при расчетах рассматриваются стационарные шумы, однако в течение длительного периода времени (день - ночь, рабочие дни - выходные) шумы могут носить нестационарный характер, т.е. изменяться во времени. Маскирующие свойства шумов проявляются тем сильнее, чем больше их превышение над полезным сигналом во всей полосе частот речевого диапазона.

Значения уровней шумов ($L_ш$), измеренные на частоте 1000 Гц в различных местах, приводятся в табл. 1.

Таблица 1. Уровни шумов, измеренные на частоте 1000Гц

Источник шума и место его измерения	Уровень шума, дБ (f=1000Гц)
Акустические шумы вне помещений	
Тихий сад	20
Тихая улица (без движения транспорта)/Двор	30-35
Шумный двор	45-50
Улица (обычный средний шум на улице)	55-60
Шумная улица с проезжей частью	60-75
Акустические шумы в помещениях	
Обычное учреждение, жилое помещение	40
Коридоры	35-40
Бухгалтерия без посетителей	30-35
Комната шумная	40-50
Комната тихая	25-30
Кабинет при одном работающем	20-25

Понятность и разборчивость речи

Разборчивостью называют относительное или процентное количество принятых специально тренированными слушателями (артикулянтами) элементов речи из общего количества переданных по тракту. Так как в качестве элементов речи применяют звуки, слоги, слова и фразы, то имеет место звуковая, слоговая, словесная и фразовая разборчивость. Объективные, измерительные оценки разборчивости речи могут производиться с помощью вычисления разборчивости формант.

По формантной разборчивости $A_Ф$ определяют слоговую S, словесную W, фразовую разборчивость и понятность речи. Зависимость между формантной $A_Ф$ (суммарной вероятностью приема формант), слоговой S и словесной W разборчивостью речи приведена в табл. 1.

Коэффициент разборчивости w определяется уровнем ощущения формант. Уровень ощущения формант $E_Ф$ определяется из выражения:

$$E_Ф = L_{пр} - L_ш, \qquad (1)$$

где:

$L_ш$ – уровень шума с внешней стороны перегородки;

$L_{пр}$ - уровень звукового давления с внешней стороны перегородки.

Для практики применение полос равной разборчивости неудобно, так как получающиеся частотные полосы нестандартны. Для каждой полосы равной разборчивости коэффициент разборчивости wi в общем случае будет разный, поэтому в акустических измерениях используются октавные или третьоктавные частотные полосы. Для простоты вычислений будем использовать значения разборчивости речи и уровни ощущения формант в октавной полосе 1000 Гц.

Минимальная формантная разборчивость $A_Ф$, при которой еще возможно понимание смысла речевого сообщения (суммарная вероятность приема формант) равна 15%, (табл. 2).

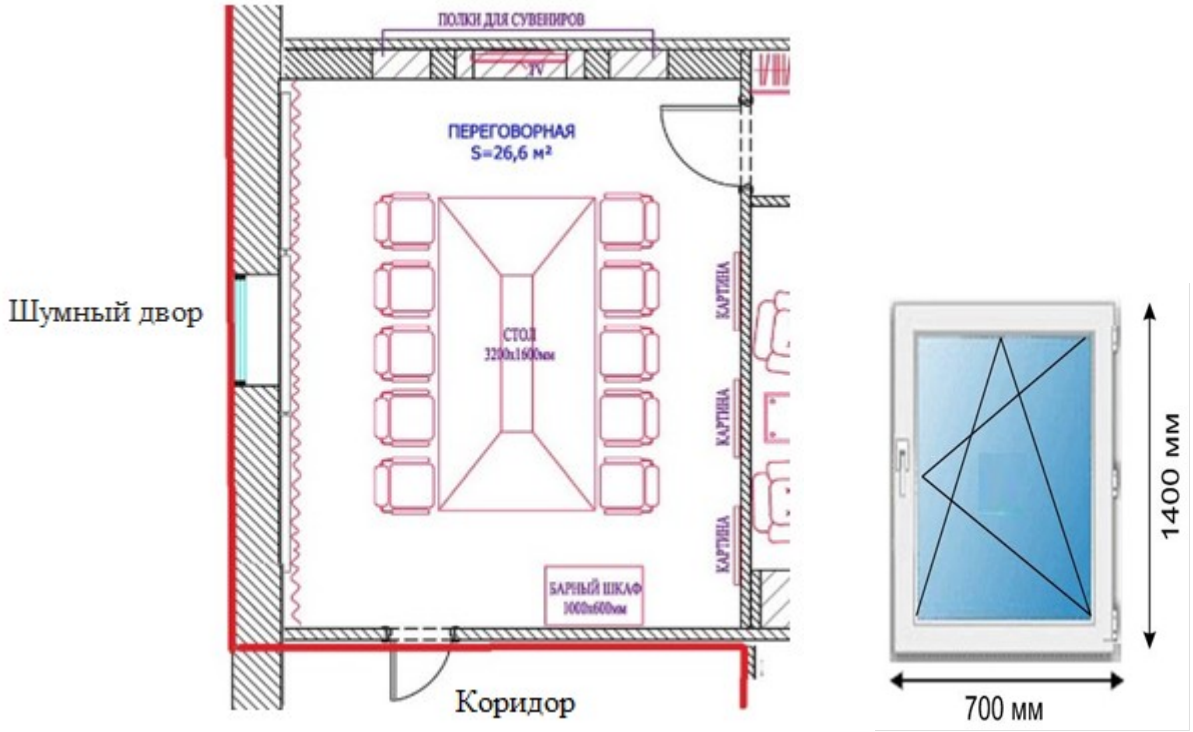
Таблица 2. Разборчивость речи и уровни ощущения формант в октавной полосе 1000 Гц

Понятность речи	Суммарная разборчивость формант $A_ф$. русск., %	Уровень ощущения формант $E_ф$, дБ

Смысл не понятен	<15	<-10
Предельно допустимая	15-22	-8…-10
Удовлетворительная	22-31	-6…-8
Хорошая	31-50	-3…-6
Отличная	=>50	=>-3

Обработка результатов.
На основании полученных результатов и рассчитанного уровня ощущения формант $E_ф$, дБ определяется суммарная разборчивость формант $А_ф$. русск., % (табл.2) и делается вывод об утечке речевой информации за пределы границ контролируемой зоны (смежный кабинет/улица/двор). Утечка возможна в случае превышения значения $А_ф$. русск., % установленного требованию защиты.

Пример расчёта
Рассмотрим возможность утечки речевых сообщений из исследуемого кабинета.



Размеры: 4х5м, h=3м.
Размер двери: 2х0,9м.

Граница контролируемой зоны показана красным. Окно выходит в шумный двор. Дверь выходит в коридор.

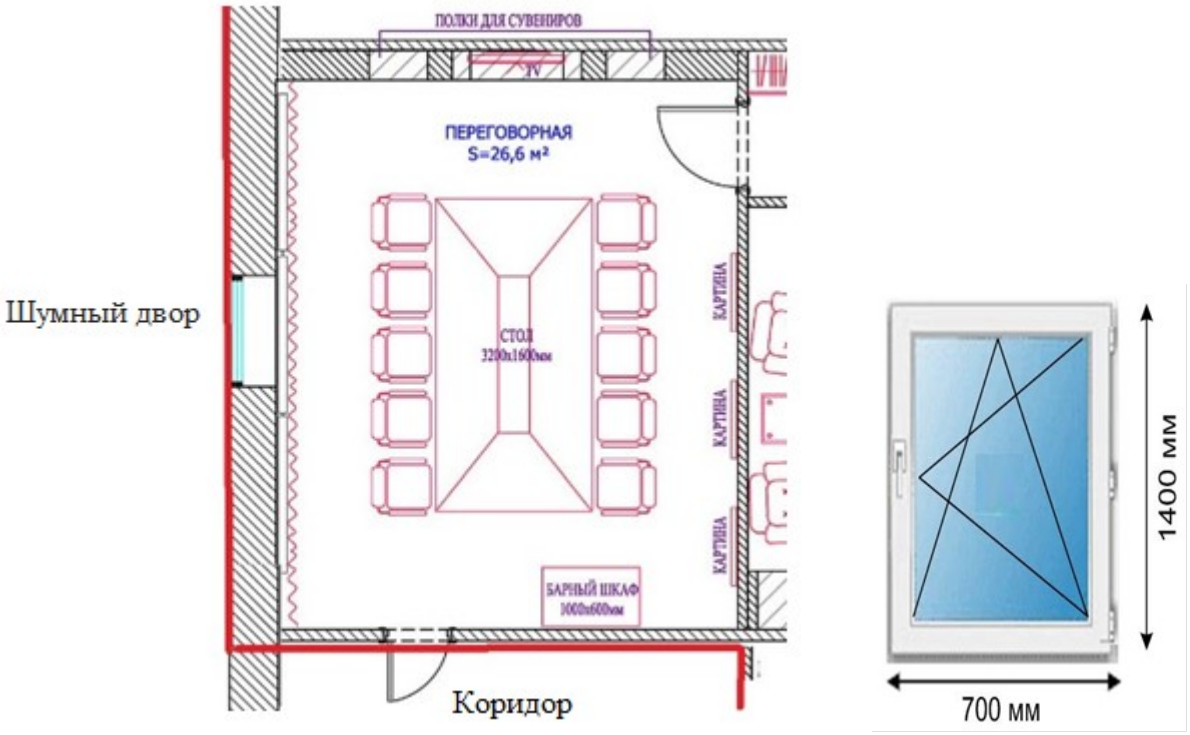
По формуле (1) определяем $L_{пр}$(дБ). Значение $L_{пад}$ - уровень речевого сигнала в контролируемом помещении, определяем по табл. 2 (выбираем максимальное значение диапазона). Источник звука – «Громкий»: 70 дБ.

В соответствии с выражением (1) определим уровни речевого сигнала за окном $L_{пр1}$ и за дверью $L_{пр2}$:

$L_{пр1}$ =70+6−39=37 дБ - за окном;

$L_{пр2}$ =70+6−25,7=51 дБ - за дверью в коридоре;

Рассмотрим возможность утечки речевых сообщений из исследуемого кабинета.



Размеры: 4х5м, h=3м.
Размер двери: 2х0,9м.
Граница контролируемой зоны показана красным.

- $L_{пр1}$ =37 дБ - за окном;
- $L_{пр2}$ =51 дБ - за дверью в коридоре;
- окно выходит в шумный двор, $L_{ш1}$ =45 дБ;
- для коридора $L_{ш2}$=35 дБ.

Так как окно выходит в шумный двор, то для определения шума подходит уровень, соответствующий 45 дБ (табл. 1), а для коридора - 35 дБ (табл. 1). При расчётах, чтобы не завысить уровень шума, будем использовать наименьшее значение предельного спектра.

Тогда по формуле (1) на среднегеометрической частоте 1000 Гц:

$E_{Ф1}=37-45=-8$ дБ - за окном;
$E_{Ф2}=41,8-35=16$ дБ - за дверью.

В соответствии с данными табл. 2:

- за окном слышимость предельно допустимая;
- за дверью слышимость отличная.

Вывод: Утечка возможна и через стену с окном и стену с дверью. Необходимы средства защиты речевой информации по акустическому каналу.

3. Задание

1) Для помещения, назначенного преподавателем (см. варианты заданий, приложение Ж), определить уровень шумов вне помещения и в помещении;
2) Определить уровень акустического сигнала перед ограждающей конструкцией и за ограждающей конструкцией. Источник звука – «Громкий».
3) Для формирования исходных данных необходимо выбрать свой вариант объекта защиты согласно порядкового номера в списке преподавателя.

4) Для помещения, назначенного преподавателем (см. варианты заданий, приложение Ж), определить уровень шума с внешней стороны перегородки (табл.1).
5) Определить разборчивость речи $А_Ф$ (табл. 2).
6) Сделать вывод об утечки речевой информации.

3. Содержание отчета:

Отчет по лабораторной работе оформляется в программной оболочке Microsoft Word (других редакторах) и предоставляется преподавателю в электронном виде с расширением «.doc».

Отчет по лабораторной работе должен состоять из следующих структурных элементов:

- титульный лист (см. Приложение А);
- вводная часть (описание методики);
- основная часть (расчеты);
- вывод.

Зашита отчета по лабораторной работе заключается в предъявлении преподавателю полученных результатов в виде файла и демонстрации полученных навыков при ответах на вопросы преподавателя.

5. Контрольные вопросы

1. Что является источником акустического сигнала в защищаемом помещении?
2. В каких единицах измеряется уровень акустического сигнала?
3. Как определяется уровень акустического сигнала за ограждающей конструкцией?
4. Каков уровень акустического шума в тихой комнате?

Литература

1. Кученков Е. Б., Музалев Е. А. Экспериментальная оценка акустической защищенности исследуемых помещений // Вопросы защиты информации. - М.: 1999., № 3.
2. Снижение шума в зданиях и жилых районах / Под ред. Осипова Г. Л., Юдина Е.Я. - М: Стройиздат, 1987.
3. Справочник проектировщика. Защита от шума / Под ред. Юдина Е. Я. - М.: Стройиздат, 1974.
4. СНИП 23-03-2003. Защита от шума.
5. Волобуев, С. Защита конфиденциальной речевой информации: простейшие методики / С. Волобуев // Системы безопасности. 2003. - №6(54).

ПРИЛОЖЕНИЕ А

Образец титульного листа

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное
образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

ОТЧЁТ

по практической работе №1

по дисциплине «Основы нформационной безопасности»

Вариант № 1

Выполнил студент гр. _____

_____

Проверил преподаватель

Калиберда И.В.

Пятигорск 2024

ПРИЛОЖЕНИЕ Б

Темы:

1. Офис торговой компании «МаксиПост». Основной функцией торговой компании является продажа средств технической защиты информации. Документы и сведения, составляющие коммерческую тайну Организации: бухгалтерские документы, планы (бизнес, логистика) текущих проектов, переписка с заказчиками, учётные записи и пароли доступа к информации.
2. Администрация компании «Аргус». Характеристика деятельности: проектирование, разработка промышленного образца НОУ-ХАО. Обеспечение безопасности конфиденциальной информации. Главным подходом предприятия является продажа мелким оптом изделий НОУ-ХАО стратегическим партнёрам.
3. Центр занятости. Осуществляет на территории муниципального района следующие функции: регистрация граждан в целях содействия в поиске подходящей работы, а также регистрация безработных граждан, оказание в соответствии с законодательством Российской Федерации следующих государственных услуг: содействие гражданам в поиске подходящей работы, а работодателям в подборе необходимых работников; информирование о положении на рынке труда; организация профессиональной ориентации граждан в целях выбора сферы деятельности (профессии), трудоустройства, профессионального обучения; психологическая поддержка безработных граждан; профессиональная подготовка, переподготовка и повышение квалификации безработных граждан, включая обучение в другой местности и т.д.
4. Компания «Артсок». Характеристика деятельности: проектирование, разработка промышленного образца НОУ-ХАО. Главным подходом предприятия является продажа мелким оптом изделий НОУ-ХАО стратегическим партнёрам.
5. Научно-производственное предприятие «Вершина». Характеристика деятельности: научные исследования в создании полезной модели, разработка промышленных образцов НОУ-ХАО. Главным подходом предприятия является продажа изделий НОУ-ХАО стратегическим партнёрам.
6. Научно-образовательный центр «Глобус». Учреждение дополнительного профессионального образования "Центр повышения квалификации специалистов по технической защите информации" с использованием нормативной документации с меткой ДСП.
7. Предприятие «Астра». Основные функции предприятия: оказание консультационных услуг предприятиям, организациям, физическим лицам по широкому кругу вопросов экономики и права (создание и регистрация фирм, маркетинговые исследования, инновации, инвестиции, диагностика проблем клиентов и др.).
8. Компания «Стик». Компания осуществляет продажу товаров народного потребления и оказание услуг покупателям для личного, семейного, домашнего или профессионального использования.
9. Коммерческая организация ООО «Кредитор». Ведет коллекторскую деятельность на предсудебном и судебном этапах. Занимается возвратом долгов юридических лиц в несудебном порядке, взыскиванием долгов в арбитражном суде, покупкой долгов.
10. Научно-внедренческая группа «Элис». Характеристика деятельности: научные исследования в создании полезной модели, разработка промышленных образцов НОУ-ХАО. Главным подходом предприятия является продажа изделий НОУ-ХАО стратегическим партнёрам.
11. Инспекция Федеральной налоговой службы. ИФНС осуществляет следующие полномочия в установленной сфере деятельности: осуществляет контроль и надзор за: соблюдением законодательства о налогах и сборах; осуществлением валютных операций резидентами и нерезидентами, не являющимися кредитными организациями; соблюдением требований к контрольно-кассовой технике, порядком и условиями ее регистрации и применения; и т.д.

12. Администрация города. Функции, выполняемые городской администрацией: разработка проектов бюджета города, планов, программ, нормативных и правовых актов Муниципального Совета, исполнение бюджета города, исполнение решений Муниципального Совета, принятых в пределах его компетенции и т.д. Вся информация, хранимая, обрабатываемая или передаваемая в рамках Администрации с использованием информационной системы, классифицирована по степени важности и критичности на следующие категории. Конфиденциальная информация: к конфиденциальной относится информация о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющая идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях, а также любая другая закрытая информация, являющаяся собственностью Администрации. При обработке этой информации необходимо соблюдать требования Федерального закона "О персональных данных", а также прочих нормативных правовых актов, регламентирующих работу с конфиденциальной информацией. Служебная информация: к служебной информации могут быть отнесены любые сведения, относящиеся к деятельности подразделений Администрации, несанкционированное распространение которых может привести к отрицательным экономическим, этическим или иным последствиям. Хранение, обработка и передача такой информации должны осуществляться в соответствии с требованиями настоящего документа. Рабочая информация: включает в себя сведения, имеющие отношение к внутренней деятельности подразделений Администрации и не относящиеся к конфиденциальной или служебной информации. При хранении, передаче и обработке такой информации необходимо обеспечить максимальный уровень ее целостности и аутентичности в соответствии с положениями настоящего документа.

13. Конструкторское бюро «Сократ». Характеристика деятельности: научные исследования в создании полезной модели, разработка промышленных образцов НОУ-ХАО. Главным подходом предприятия является продажа изделий НОУ-ХАО стратегическим партнёрам.

14. Акционерное общество «Торг-Сервис». Компания осуществляет продажу товаров народного потребления и оказание услуг покупателям для личного, семейного, домашнего или профессионального использования.

15. Муниципальное Унитарное Предприятие "Новый город". МУП «Новый город» занимается строительством, капитальным ремонтом и реконструкцией объектов капитального строительства; ведёт работы по инженерным изысканиям, влияющим на безопасность капитального строительства объектов; подготавливает проектную документацию, необходимую для возведения сооружений капитального строительства. Для предприятия определен перечень сведений конфиденциального характера, в том числе сведения о порядке и состоянии организации защиты коммерческой тайны и сведения, содержащие персональные данные работников организации персональные данные партнеров предприятия.

16. Научно-производственное предприятие «Вектор». Компания осуществляет продажу товаров народного потребления и оказание услуг покупателям для личного, семейного, домашнего или профессионального использования.

17. Компания "Служба оконного сервиса". Предприятие занимается продажей, установкой и ремонтом пластиковых окон. Для предприятия определен перечень сведений конфиденциального характера, в том числе сведения о порядке и состоянии организации защиты коммерческой тайны и сведения, содержащие персональные данные работников организации персональные данные партнеров предприятия.

ПРИЛОЖЕНИЕ В

Шаблон политики ИБ

УТВЕРЖДЕНА
приказом {Название Организации}
от «___» _____20__г. № ___

Политика информационной безопасности в {Название Организации}

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая политика информационной безопасности (далее - Политика) утверждается руководителем {Название Организации} и определяет мероприятия, процедуры и правила по защите информации в информационных системах {Название Организации}.

1.2. Положения настоящей Политики распространяются на следующие информационные системы {Название Организации}:

- ГИС «ИС»;
- ИСПДн «Бухгалтерия и кадры»;
- ИС «Делопроизводство».

1.3. Положения настоящей Политики обязательны к исполнению для всех пользователей, указанных в п. 1.2 информационных систем (далее - Пользователи), а также для администраторов информационной безопасности (далее АИБ) и системных администраторов (далее - Администраторы).

1.4. Защищаемые информационные ресурсы Организации.

В учреждении должны быть выявлены и оценены с точки зрения их важности все ресурсы.
Для всех ценных ресурсов должен быть составлен реестр (перечень). Благодаря информации о ресурсах Учреждения реализуется защита информации, степень которой соразмерна ценности и важности ресурсов.
В ИС Учреждения присутствуют следующие типы ресурсов:

- информационные ресурсы, содержащие конфиденциальную информацию, и/или сведения ограниченного доступа, в том числе информацию о финансовой деятельности Учреждения;
- открыто распространяемая информация, необходимая для работы Учреждения, независимо от формы и вида её представления;
- информационная инфраструктура, включая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации,
- системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

Для каждого ресурса должен быть назначен владелец, который отвечает за соответствующую классификацию информации и ресурсов, связанных со средствами обработки информации, а также за назначение и периодическую проверку прав доступа и категорий, определённых политиками управления доступа.
В соответствии с указом Президента Российской Федерации № 188 от 6 марта 1997 года к сведениям конфиденциального характера (защищаемой информации) в {Название Организации} относятся:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за

исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее) {оставить нужное};
- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна) {только для госов};
- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

1.5. Целями настоящей Политики являются:

- обеспечение конфиденциальности, целостности, доступности защищаемой информации;
- предотвращение утечек защищаемой информации;
- мониторинг событий безопасности и реагирование на инциденты безопасности;
- нейтрализация актуальных угроз безопасности информации;
- выполнение требований действующего законодательства по защите информации.

1.6. В настоящей Политике используются термины и определения, установленные законодательством Российской Федерации об информации, информационных технологиях и о защите информации, а также термины и определения, установленные национальными стандартами в области защиты информации.

1.7. Настоящая Политика разработана с учетом положений следующих законодательных и нормативно-правовых актов:

- Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информатизации и защите информации»;
- Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»;
- «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;
- «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 года;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;
- методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утверждённые приказом ФСБ России № 378 от 10.07.2014;
- «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом ФСБ от 9 февраля 2005 №66;
- «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты

информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 №152.

1.8. Ответственность за обеспечение ИБ

Ответственность за разработку мер и контроль обеспечения защиты информации несёт АИБ.

Для непосредственной организации и эффективного функционирования системы обеспечения информационной безопасности в Учреждении функции обеспечения ИБ возложены на отдел {название отдела по БИ}. На это подразделение возлагается решение следующих основных задач:

- проведение в жизнь Политики ИБ;
- определение требований к защите информации;
- организация мероприятий и координация работ всех подразделений по вопросам комплексной защиты информации;
- контроль и оценка эффективности принятых мер и применяемых средств защиты;
- оказание методической помощи сотрудникам в вопросах обеспечения информационной безопасности;
- регулярная оценка и управление рисками информационной безопасности в соответствии с установленными процедурами в области управления рисками;
- выбор и внедрение средств защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства обеспечения СУИБ;
- обеспечение минимально-необходимого доступа к информационным ресурсам, основываясь на требованиях бизнес-процессов;
- информирование, обучение и повышение квалификации работников Учреждения в сфере информационной безопасности;
- расследования инцидентов информационной безопасности;
- сбор, накопление, систематизация и обработка информации по вопросам информационной безопасности;
- обеспечение необходимого уровня отказоустойчивости ИТ-сервисов и доступности данных для подразделений.

Для решения задач, возложенных на отдел НАЗВАНИЕ, его сотрудники имеют следующие права:

- определять необходимость и разрабатывать нормативные документы, касающиеся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность пользователей информационной системы в указанной области;
- получать информацию от пользователей информационных систем Учреждения по любым аспектам применения информационных технологий в Учреждении;
- участвовать в проработке технических решений по вопросам обеспечения безопасности информации при проектировании и разработке новых информационных технологий;
- участвовать в испытаниях разработанных информационных технологий по вопросам оценки качества реализации требований по обеспечению безопасности информации;
- контролировать деятельность пользователей по вопросам обеспечения ИБ;
- готовить предложения руководству по обеспечению требований ИБ.

ПРИЛОЖЕНИЕ Г

Шаблон 1

Политика управления рисками.

В учреждении должны быть определены требования к безопасности путём методической оценки рисков. Оценки рисков должны выявить, определить количество и расположить по приоритетам риски в соответствии с критериями принятия рисков и бизнес-целями учреждения. Результаты оценки должны определять соответствующую реакцию руководства, приоритеты управления рисками ИБ и набор механизмов контроля для защиты от этих рисков.

Оценка рисков предполагает системное сочетание анализа рисков и оценивания рисков.

Кроме того, оценка рисков и выбор механизмов контроля должны производиться периодически, чтобы:

- учесть изменения бизнес-требований и приоритетов;
- принять во внимание новые угрозы и уязвимости;
- убедиться в том, что реализованные средства сохранили свою эффективность.

Перед обработкой каждого риска Учреждение должно выбрать критерии для определения возможности принятия этого риска. Риск может быть принят, если его величина достаточно мала и стоимость обработки нерентабельна для Учреждения. Такие решения должны регистрироваться.

Для каждого из оцененных рисков должно приниматься одно из решений по его обработке:

- применение соответствующих механизмов контроля для уменьшения величины риска до приемлемого уровня;
- сознательное и объективное принятие риска, если он точно удовлетворяет Политике Учреждения и критериям принятия рисков;
- уклонение от риска путём недопущения действий, могущих быть его причиной;
- передача рисков другой стороне (аутсорсинг, страхование и т.п.).

В процессе обработки должны быть выбраны меры и средства контроля и управления для снижения, сохранения, предотвращения или переноса рисков, а также определен план обработки рисков.

Варианты обработки риска должны выбираться исходя из результатов оценки риска, предполагаемой стоимости реализации этих вариантов и их ожидаемой эффективности. Должны реализовываться такие варианты, при которых значительное снижение риска может быть достигнуто при относительно небольших затратах. Дополнительные варианты повышения эффективности могут быть неэкономичными, и необходимо принимать решение о целесообразности их применения.

Неблагоприятные последствия рисков необходимо снижать до разумных пределов независимо от каких-либо абсолютных критериев.

Методика оценки риска приведена в приложении 1. Организация должна хранить документированную информацию о результатах проведенных оценок рисков информационной безопасности.

Шаблон 2

Политика безопасности персонала

Роли и обязанности по обеспечению безопасности информационных ресурсов, описанные в соответствии с Политикой ИБ Учреждения, должны быть доведены до сотрудника при трудоустройстве и внесены в его должностные обязанности. Сюда должны входить как общие обязанности по реализации и поддержке политики безопасности, так и конкретные обязанности по защите ресурсов и по выполнению конкретных операций, связанных с безопасностью.

1. Условия найма

Все принимаемые на работу сотрудники должны одобрить и подписать свои трудовые договоры, в которых устанавливается их ответственность за ИБ. В договор должно быть включено согласие сотрудника на проведение контрольных мероприятий со стороны Учреждения по проверке выполнения требований ИБ, а также обязательства по неразглашению конфиденциальной информации. В договоре должны быть описаны меры, которые будут приняты в случае несоблюдения сотрудником требований ИБ.

Обязанности по обеспечению ИБ должны быть включены в должностные инструкции каждого сотрудника Учреждения.

Все принимаемые сотрудники должны быть ознакомлены под роспись с перечнем информации, ограниченного доступа, с установленным режимом с ней и с мерами ответственности за нарушение этого режима.

При предоставлении сотруднику доступа к ИС Учреждения он должен ознакомиться под роспись с инструкцией пользователя ИС.

2. Ответственность руководства

Руководство Учреждения должно требовать от всех сотрудников, подрядчиков и пользователей сторонних организаций принятия мер безопасности в соответствии с установленными в Учреждении политиками и процедурами.

Уполномоченные руководством Учреждения сотрудники имеют право в установленном порядке, без уведомления пользователей, производить проверки:

- Выполнения действующих инструкций по вопросам ИБ;
- Данных, находящихся на носителях информации;
- Порядка использования сотрудниками информационных ресурсов;
- Содержания служебной переписки.

3. Обучение ИБ

Все сотрудники должны проходить периодическую подготовку в области политики и процедур ИБ, принятых в Учреждении.

4. Завершение или изменения трудовых отношений

При увольнении все предоставленные сотруднику права доступа к ресурсам ИС должны быть удалены. При изменении трудовых отношений удаляются только те права, необходимость в которых отсутствует в новых отношениях.

Шаблон 3

Политика физической безопасности

1. Защищённые области

Средства обработки информации, поддерживающие критически важные и уязвимые ресурсы Учреждения, должны быть размещены в защищённых областях. Такими средствами являются: серверы, магистральное телекоммуникационное оборудование, телефонные станции, кроссовые панели, оборудование, обеспечивающее обработку и хранение конфиденциальной информации. Перечень помещений, в которых разрешена работа с

ресурсами ГИС «Бухгалтерия и кадры», в которых размещены технические средства ГИС, а также перечень лиц, допущенных в эти помещения приведен в Приложении № 3.
Защищённые области должны обеспечиваться соответствующими средствами контроля доступа, обеспечивающим возможность доступа только авторизованного персонала.
Запрещается приём посетителей в помещениях, когда осуществляется обработка информации ограниченного доступа.
Для хранения служебных документов и машинных носителей с защищаемой информацией помещения снабжаются сейфами, металлическими шкафами или шкафами, оборудованными замком.
Помещения должны быть обеспечены средствами уничтожения документов.

2. Области общего доступа
Места доступа, через которые неавторизованные лица могут попасть в помещения Учреждения, должны контролироваться и, если это возможно, должны быть изолированы от средств обработки информации с целью предотвращения несанкционированного доступа.

3. Вспомогательные службы
Все вспомогательные службы, такие как электропитание, водоснабжение, канализация, отопление, вентиляция и кондиционирование воздуха должны обеспечивать гарантированную и устойчивую работоспособность компонентов ИС Учреждения.

4. Утилизация или повторное использование оборудования
Со всех носителей информации, которыми укомплектовано утилизируемое оборудование, должны гарантированно удаляться все конфиденциальные данные и лицензионное ПО. Отсутствие защищаемой информации на носителях должно быть проверено отделом ИС СМТ Учреждения, о чём должна быть сделана отметка в акте списания.

5. Перемещение имущества
Оборудование, информация или ПО должны перемещаться за пределы Учреждения только при наличии письменного разрешения руководства. Сотрудники, имеющие право перемещать оборудование и носители информации за пределы Учреждения должны быть чётко определены. Время перемещения оборудования за пределы Учреждения и время его возврата должны регистрироваться.

Шаблон 3

Политика контроля доступа
Основными пользователями информации в информационной системе Учреждения являются сотрудники структурных подразделений. Уровень полномочий каждого пользователя определяется индивидуально. Каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходимо работать в соответствии с должностными обязанностями.
Допуск пользователей к работе с информационными ресурсами должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться в установленном порядке, согласно регламента предоставления доступа пользователей.
Каждому пользователю, допущенному к работе с конкретным информационным активом Учреждения, должно быть сопоставлено персональное уникальное имя (учётная запись пользователя), под которым он будет регистрироваться и работать с ИА.
В случае производственной необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имён (учётных записей).

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

В общем случае запрещено создавать и использовать общую пользовательскую учётную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или организации труда (например, посменное дежурство), использование общей учётной записи должно сопровождаться отметкой в журнале учёта машинного времени, которая должна однозначно идентифицировать текущего владельца учётной записи в каждый момент времени. Одновременное использование одной общей пользовательской учётной записи разными пользователями запрещено.

Регистрируемые учётные записи подразделяются на:

- Пользовательские – предназначенные для аутентификации пользователей ИР Учреждения;
- Системные – используемые для нужд операционной системы;
- Служебные – предназначенные для функционирования отдельных процессов или приложений.

Системные учётные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.

Служебные учётные записи используются только для запуска и работы сервисов или приложений.

Использование системных или служебных учётных записей для регистрации пользователей в системе категорически запрещено.

Процедуры регистрации и блокирования учётных записей пользователей должны применяться с соблюдением следующих правил:

- использование уникальных идентификаторов (ID) пользователей для однозначного определения и сопоставления личности с совершёнными ей действиями;
- использование групповых ID разрешать только в случае, если это необходимо для выполнения задачи;
- предоставление и блокирование прав должны быть санкционированы и документированы;
- предоставление прав доступа к ИР, только после согласования с владельцем данного ИР;
- регистрация и блокирование учётных записей допускается с отдельного разрешения руководства Учреждения;
- уровень предоставленных полномочий должен соответствовать производственной необходимости и настоящей Политике и не ставить под угрозу разграничение режимов работы;
- согласование изменения прав доступа с отделом ИС СМТ;
- документальная фиксация назначенных пользователю прав доступа;
- ознакомление пользователей под подпись с письменными документами, в которых регламентируются их права доступа;
- предоставление доступа с момента завершения процедуры регистрации;
- обеспечение создания и поддержания формального списка всех пользователей, зарегистрированных для работы с ИР или сервисом;
- немедленное удаление или блокирование прав доступа пользователей, сменивших должность, форму занятости или уволившихся из Учреждения;
- аудит ID и учетных записей пользователей на наличие неиспользуемых, их удаление и блокировка;
- обеспечение того, чтобы лишние ID пользователей не были доступны другим пользователям;

- обеспечить возможность предоставления пользователям доступа в соответствии с их должностями, основанными на производственных требованиях, путем суммирования некоторого числа прав доступа в типовые профили доступа пользователей.

1. Управление привилегиями

Доступ сотрудника к информационным ресурсам Учреждения должен быть санкционирован руководителем структурного подразделения, в котором числится согласно штатному расписанию данный сотрудник, и владельцами соответствующих информационных ресурсов. Управление доступом осуществляется в соответствии с установленными процедурами.

Наделение привилегиями и их использование должно быть строго ограниченным и управляемым. Распределение привилегий должно управляться с помощью процесса регистрации этих привилегий. Должны быть рассмотрены следующие этапы:

- должны быть идентифицированы привилегии доступа, связанные с каждым системным продуктом, например, с операционной системой, системой управления базой данных и каждым приложением, а также пользователи, которым они должны быть предоставлены;
- привилегии должны предоставляться пользователям на основании «производственной необходимости» и только на период времени, необходимый для достижения поставленных целей, например, привилегии, минимально необходимые для выполнения их функциональных обязанностей, только тогда, когда эти привилегии необходимы;
- должен быть обеспечен процесс санкционирования всех предоставленных привилегий и создание отчетов по ним, привилегии нельзя предоставлять до завершения процесса их регистрации;
- уникальные привилегии должны присваиваться на другой ID пользователя, не тот, который используется при обычной работе пользователя.

Контроль и периодический пересмотр прав доступа пользователей к информационным ресурсам Учреждения осуществляется в процессе аудита ИБ в соответствии с Правилами аудита ИБ и установленными процедурами.

2. Управление паролями

Пароли – средство проверки личности пользователя для доступа к ИС или сервису, обеспечивающее идентификацию и аутентификацию на основе сведений, известных только пользователю.

Предоставление паролей должно контролироваться посредством официальной процедуры, отвечающей следующим требованиям:

- все пользователи должны быть ознакомлены под роспись с требованием сохранения в тайне личных и групповых паролей;
- при наличии возможности, необходимо настроить систему таким образом, чтобы при первом входе пользователя с назначенным ему временным паролем система сразу же требовала его сменить;
- временные пароли должны назначаться пользователю только после его идентификации;
- необходимо избегать передачи паролей с использованием третьих лиц или незашифрованной электронной почтой;
- временные пароли не должны быть угадываемыми и повторяющимися от пользователя к пользователю;
- пользователь должен подтвердить получение пароля;
- пароли должны храниться в электронном виде только в защищенной форме;
- назначенные производителем ПО пароли должны быть изменены сразу после завершения инсталляции;
- необходимо установить требования к длине пароля, набору символов и числу попыток ввода;
- необходимо изменять пароля пользователя не реже одного раза в 90 дней.

При необходимости можно рассмотреть возможность использования других технологий идентификации и аутентификации пользователей, в частности, биометрических технологий, проверки подписи и аппаратных средств (смарт-карты, e-Token/ruToken, чипы и т.п.).

3. Контроль прав доступа

Чтобы обеспечить эффективный контроль доступа необходимо ввести официальный процесс регулярной проверки прав доступа пользователей, отвечающий следующим требованиям:

- права доступа пользователей должны проверяться через регулярные интервалы (не реже одного раза в полгода), а также после внесения каких-либо изменений в ИС;
- права доступа пользователей должны проверяться и переназначаться при изменении их должностных обязанностей в Учреждении, а также при переходе с одной работы на другую в пределах Учреждения;
- проверка прав пользователей, имеющих особые привилегии для доступа в систему, должна проводиться чаще (не реже одного раза в 3 месяца);
- необходимо регулярно проверять адекватность назначенных привилегий, во избежание получения кем-либо из пользователей излишних прав;
- изменение привилегированных учетных записей должно протоколироваться.

Контроль над выполнением процедур управления доступом пользователей должен включать:

- контроль над добавлением, удалением и изменением идентификаторов, аутентификационных данных и иных объектов идентификации;
- проверку подлинности пользователей перед сменой паролей;
- немедленное блокирование прав доступа при увольнении;
- блокирование учётных записей, неактивных более 45 дней;
- включение учётных записей, используемых поставщиками для удалённой поддержки, только на время выполнения работ;
- отслеживание удалённых учётных записей, используемых поставщиками, во время работ;
- предотвращение повторного использования идентификатора пользователя и (или) устройства в течение не менее трёх лет;
- ознакомление с правилами и процедурами аутентификации всех пользователей, имеющих доступ к сведениям ограниченного распространения;
- использование механизмов аутентификации при доступе к любой базе данных, содержащей сведения ограниченного распространения, в том числе доступе со стороны приложений, администраторов и любых других пользователей;
- разрешение запросов и прямого доступа к базам данных только для администраторов баз данных;
- блокирование учётной записи на период равный 30 минутам или до разблокировки учётной записи администратором;
- блокирование учетных записей пользователей при выявлении по результатам мониторинга (просмотра, анализа) журналов регистрации событий безопасности действий пользователей, которые отнесены оператором к событиям нарушения безопасности информации.

4. Использование паролей

Идентификатор и пароль пользователя в ИС являются учётными данными, на основании которых сотруднику Учреждения предоставляются права доступа, протоколируются производимые им в системе действия и обеспечивается режим конфиденциальности, обрабатываемой (создаваемой, передаваемой и хранимой) сотрудником информации.

Не допускается использование различными пользователями одних и тех же учётных данных.

Первоначальное значение пароля учетной записи пользователя устанавливает Администратор безопасности.

Личные пароли устанавливаются первый раз сотрудниками отдела ИС СМТ. После первого входа в систему и в дальнейшем пароли выбираются пользователями автоматизированной системы самостоятельно с учетом установленных требований
Сотруднику запрещается:

- сообщать свой пароль кому-либо;
- указывать пароль в сообщениях электронной почты;
- хранить пароли, записанные на бумаге, в легко доступном месте;
- использовать тот же самый пароль, что и для других систем (например, домашний интернет провайдер, бесплатная электронная почта, форумы и т.п.);
- использовать один и тот же пароль для доступа к различным корпоративным ИС.

Вход пользователя в систему не должен выполняться автоматически.
Учреждение оставляет за собой право:

- осуществлять периодическую проверку стойкости паролей пользователей, используемых сотрудниками для доступа к ИС;
- принимать меры дисциплинарного характера к сотрудникам, нарушающим положения настоящей политики.

5. Пользовательское оборудование, оставляемое без присмотра
Пользователи должны обеспечивать необходимую защиту оборудования, остающегося без присмотра. Все пользователи должны быть осведомлены о требованиях ИБ и правилах защиты остающегося без присмотра оборудования, а также о своих обязанностях по обеспечению этой защиты.

6. Политика чистого стола
Сотрудники Учреждения обязаны:

- сохранять известные им пароли в тайне;
- закрывать активные сеансы по завершении работы, если только их нельзя защитить подходящим блокирующим механизмом, например, защищённый паролем хранитель экрана;
- по завершении сеанса выходить из системы у универсальных ЭВМ, серверов и офисных ПК.

Запрещается вести запись паролей (например, на бумаге, в программном файле или в карманном устройстве), за исключением случаев, когда запись может храниться безопасно, а метод хранения был утверждён.
Документы и носители с конфиденциальной информацией должны убираться в запираемые места (сейфы, шкафы и т.п.), особенно при уходе с рабочего места.
Компьютеры и терминалы должны быть оставлены в состоянии выполненного выхода из системы, когда они находятся без присмотра.
Вход пользователя в систему не должен выполняться автоматически.

Документы, содержащие конфиденциальную информацию, должны изыматься из печатающих устройств немедленно.
В конце рабочего дня сотрудник должен привести в порядок письменный стол и убрать все офисные документы в запираемый шкаф или сейф.
Для утилизации конфиденциальных документов, должны использоваться уничтожители бумаги.
По окончании рабочего дня и в случае длительного отсутствия на рабочем месте необходимо запирать на замок все шкафы и сейфы.

7. Мобильное компьютерное оборудование

При использовании мобильных средств (например, ноутбуков, планшетов и мобильных телефонов) необходимо соблюдать особые меры предосторожности, чтобы не допустить компрометацию информации, принадлежащей Учреждению. Необходимо принять официальную политику, учитывающую риск, связанный с использованием мобильных компьютеров, и в частности с работой в незащищённой среде.

Шаблон 4

Политика допустимого использования информационных ресурсов

Общие обязанности пользователя:

- при работе с ПО руководствоваться нормативной документацией (руководством пользователя);
- обращаться в службу поддержки пользователей или к специалистам, назначенными ответственными за системное администрирование и информационную безопасность, по всем техническим вопросам, связанным с работой в корпоративной ИС (подключение к корпоративной ИС/домену, инсталляция и настройка ПО, удаление вирусов, предоставление доступа в сеть Интернет и к внутренним сетевым ресурсам, ремонт и техническое обслуживание и т.п.), а также за необходимой методологической/консультационной помощью по вопросам применения технических и программных средств корпоративной ИС;
- знать признаки правильного функционирования установленных программных продуктов и средств защиты информации;
- минимизировать вывод на печать обрабатываемой информации.

Пользователю запрещено производить несанкционированное распространение справочной информации, которая становится доступна при подключении к корпоративной ИС Учреждения.

1. Использование ПО

На АРМ <название организации> допускается использование только лицензионного программного обеспечения, утверждённого в перечне разрешённого программного обеспечения.

Запрещено незаконное хранение на жестких дисках АРМ <название организации> информации, являющейся объектом авторского права (ПО, фотографии, музыкальные файлы, игры, и т.д.).

Решение о приобретении и установке программного обеспечения, необходимого для реализации медицинских, финансовых, административно-хозяйственных и других задач принимает <должность ответственного> по представлении начальника <название ответственного отдела>.

Документы, подтверждающие покупку программного обеспечения, хранятся в бухгалтерии на протяжении всего времени использования лицензии, копии указанных документов вместе с лицензионными соглашениями на ПО, ключами защиты ПО и дистрибутивами хранятся в <название ответственного отдела>.

Пользователи АРМ не имеют права удалять, изменять, дополнять, обновлять программную конфигурацию на АРМ <название организации>. Указанные работы, а так же работы по установке, регистрации и активации приобретённого лицензионного ПО могут быть выполнены только сотрудниками <название ответственного отдела>.

Сведения о вновь приобретённом программном обеспечении должны быть внесены в перечень разрешённого программного обеспечения.

Перечень разрешенного программного обеспечения в ГИС «Бухгалтерия и кадры» определен в Приложении № 4 к настоящей Политике.

2. Использование АРМ и ИС

К работе в ИС Учреждения допускаются лица, назначенные на соответствующую должность и прошедшие инструктаж по вопросам информационной безопасности.

Каждому сотруднику Учреждения, которому необходим доступ к ИР в рамках его должностных обязанностей, выдаются под роспись необходимые средства автоматизации. Ответственность по установке и поддержке всех компьютерных систем, функционирующих в Учреждении, возложена на отдел ИС СМТ.

Каждый сотрудник Учреждения, обеспеченный АРМ, получает персональное сетевое имя, пароль, адрес электронной почты и личный каталог в сети, который предназначен для хранения рабочих файлов.

Работа в ИС сотрудникам разрешена только на закреплённых за ними АРМ, в определённое время и только с разрешенным программным обеспечением и сетевыми ресурсами.

Все АРМ, установленные в Учреждении, имеют унифицированный набор офисных программ, предназначенных для получения, обработки и обмена информацией, определённый в стандарте рабочих мест Учреждения. Изменение установленной конфигурации возможно после внесения соответствующих поправок в стандарт рабочих мест или по служебной записке, согласованной с отделом ИС СМТ. Комплектация персональных компьютеров аппаратными и программными средствами, а также расположение компьютеров контролируется отделом ИС СМТ.

Самостоятельная установка программного обеспечения на АРМ запрещена. Установка и удаление любого программного обеспечения производится только сотрудниками отдела ИС СМТ.

В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться в отдел ИС СМТ.

Сотрудники отдела ИС СМТ имеют право осуществлять контроль над установленным на компьютере программным обеспечением, и принимать меры по ограничению возможностей несанкционированной установки программ.

Передача документов внутри Учреждения производится только посредством общих папок, а также средствами электронной почты.

При работе в ИС Учреждения сотрудник обязан:

- знать и выполнять требования внутренних организационно-распорядительных документов Учреждения;
- использовать ИС и АРМ Учреждения исключительно для выполнения своих служебных обязанностей;
- ставить в известность отдел ИС СМТ о любых фактах нарушения требований ИБ;
- ставить в известность отдел ИС СМТ о любых фактах сбоев ПО, некорректного завершения значимых операций, а также повреждения технических средств;
- незамедлительно выполнять предписания отдела ИС СМТ Учреждения.
- Предоставлять АРМ сотрудникам отдела ИС СМТ для контроля;
- При необходимости прекращения работы на некоторое время корректно закрывать все активные задачи, блокировать АРМ;
- В случае необходимости продолжения работы по окончании рабочего дня проинформировать об этом отдел ИС СМТ.

При использовании ИС Учреждения запрещено:

- использовать АРМ и ИС в личных целях;
- отключать средства управления и средства защиты, установленные на рабочей станции;
- передавать:
- конфиденциальную информацию за исключением случаев, когда это входит в служебные обязанности и способ передачи является безопасным, согласованным с отделом ИС СМТ;

- информацию, файлы или ПО, способные нарушить или ограничить функциональность любых программных и аппаратных средств, а также ссылки на вышеуказанные объекты;
- угрожающую, клеветническую, непристойную информацию;
- самовольно вносить изменения в конструкцию, конфигурацию, размещение АРМ и других узлов ИС Учреждения;
- предоставлять сотрудникам Учреждения (за исключением администраторов ИС и ИБ) и третьим лицам доступ к своему АРМ;
- запускать на АРМ ПО, не входящее в Реестр разрешенного к использованию ПО;
- защищать информацию, способами, не согласованными с отделом ИС СМТ заранее;
- самостоятельно подключать рабочую станцию и прочие технические средства к корпоративной ИС Учреждения;
- осуществлять поиск средств и путей повреждения, уничтожения технических средств и ресурсов ИС или осуществлять попытки несанкционированного доступа к ним;
- использовать для выполнения служебных обязанностей локальные (не доменные) учетные записи АРМ.

Информация о посещаемых ресурсах ИС протоколируется и, при необходимости, может быть представлена Руководителям структурных подразделений, а также Руководству Учреждения.

Все электронные сообщения и документы в электронном виде, передаваемые посредством ИС Учреждения подлежат обязательной проверке на отсутствие вредоносного ПО.

3. Использование ресурсов локальной сети

Для выполнения своих служебных обязанностей каждый сотрудник обеспечивается доступом к соответствующим информационным ресурсам. Информационными ресурсами являются каталоги и файлы, хранящиеся на дисках серверов Учреждения, базы данных, электронная почта.

Основными рабочими каталогами являются личные каталоги сотрудников и каталоги подразделений, созданные в соответствии с особенностями их работы. Доступ сотрудников к ресурсам сети осуществляется согласно матрицы доступа. Временное расширение прав доступа осуществляется отделом ИС СМТ Учреждения в соответствии с Порядком предоставления (изменения) полномочий пользователя.

4. Обработка конфиденциальной информации

При обработке конфиденциальной информации сотрудники обязаны:

- знать и выполнять требования Инструкции по работе с конфиденциальной информацией;
- при необходимости размещать конфиденциальную информацию на открытом ресурсе корпоративной сети Учреждения применять средства защиты от неавторизованного доступа;
- размещать экран монитора таким образом, чтобы исключить просмотр обрабатываемой информации посторонними лицами;
- не отправлять на печать конфиденциальные документы, если отсутствует возможность контроля вывода на печать и изъятия отпечатанных документов из принтера сразу по окончании печати;
- обязательно проверять адреса получателей электронной почты на предмет правильности их выбора;
- не запускать исполняемые файлы на съемных накопителях, полученные не из доверенного источника;
- не передавать конфиденциальную информацию по открытым каналам связи, кроме сетей корпоративной ИС;
- не оставлять без личного присмотра на рабочем месте или где бы то ни было электронные носители информации (CD/DVD – диски, Flash – устройства и пр.), а также распечатки из принтера или бумажные копии документов, содержащие конфиденциальную информацию.

5. Использование электронной почты

Электронная почта используется для обмена в рамках ИС Учреждения и общедоступных сетей информацией в виде электронных сообщений и документов в электронном виде.

Для обеспечения функционирования электронной почты допускается применение ПО, входящего в реестр разрешённого к использованию ПО.

При работе с корпоративной электронной почтой Учреждения пользователь должен учитывать:

- электронная почта не является средством гарантированной доставки отправленного сообщения до адресата;
- электронная почта не является средством передачи информации, гарантирующим конфиденциальность передаваемой информации (передачу конфиденциальной информации вне локальной сети Учреждения необходимо осуществлять только в зашифрованном виде);
- электронная почта не является средством передачи информации, гарантированно идентифицирующим отправителя сообщения.

Организацией и обеспечением порядка работы электронной почты в Учреждении занимается отдел ИС СМТ.

Каждый сотрудник Учреждения получает почтовый адрес вида name@er76.ru в домене Учреждения. Адрес электронной почты выдаётся сотрудником отдела ИС СМТ при начальной регистрации пользователя в домене Учреждения.

Корпоративная электронная почта Учреждения предназначена исключительно для использования в служебных целях.

Функционирование электронной почты обеспечивается оборудованием, каналами связи и иными ресурсами, принадлежащими Учреждению. Все почтовые сообщения, переданные или принятые с использованием корпоративной электронной почты принадлежат Учреждению и являются неотъемлемой частью его производственного процесса.

Любые сообщения корпоративной электронной почты могут быть прочитаны, использованы в интересах Учреждения либо удалены уполномоченными сотрудниками Учреждения.

Пользователям корпоративной электронной почты Учреждения запрещено вести частную переписку с использованием средств корпоративной электронной почты Учреждения. К частной переписке относится переписка, не связанная с исполнением сотрудником своих должностных обязанностей.

Использование корпоративной электронной почты Учреждения для частной переписки сотрудником, надлежащим образом, ознакомленным с данной Политикой, является нарушением трудовой дисциплины Учреждения. Подписываясь в ознакомлении с настоящей Политикой, сотрудник даёт согласие на ознакомление и иное использование в интересах Учреждения его переписки, осуществляемой с использованием корпоративной электронной почты, и соглашается с тем, что любое использование его переписки, осуществляемой с использованием корпоративной электронной почты, не может рассматриваться как нарушение тайны связи.

Каждый сотрудник Учреждения имеет право на просмотр либо иное использование в интересах Учреждения сообщений корпоративной электронной почты, которые направлены или получены им, соответственно, с его или на его корпоративный электронный адрес.

Использование сообщений корпоративной электронной почты осуществляется уполномоченными сотрудниками Учреждения в соответствии с их функциями, определёнными в данной Политике и в иных локальных нормативных актах Учреждения. Просмотр и иное использование сообщений электронной почты в интересах Учреждения осуществляется сотрудниками Учреждения в целях обеспечения защиты конфиденциальных сведений, обеспечения нормальной работоспособности системы электронной почты, в рамках обслуживания сервисов электронной почты, при выполнении ручной пересылки сообщений,

приходящих на корпоративные электронные адреса Учреждения сотрудникам или группам сотрудников, а также по мотивированным запросам прямых или непосредственных руководителей любых сотрудников, чью почту необходимо использовать в интересах Учреждения.
Использование сообщений корпоративной электронной почты в интересах Учреждения, в том числе ознакомление с содержанием сообщений, осуществляется в соответствии с правами доступа к информации, установленными внутренними Положениями о конфиденциальной информации и иными правовыми актами, регламентирующими порядок обращения с информацией ограниченного доступа.
Исходящие электронные сообщения сотрудников Учреждения должны содержать следующие поля:

- адрес получателя;
- тема электронного сообщения;
- текст электронного сообщения (вложенные файлы);
- подпись отправителя;
- предупреждение о служебном характере сообщения и его конфиденциальности.

6. Работа в сети

Доступ к сети Интернет предоставляется сотрудникам Учреждения в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.
Для доступа сотрудников Учреждения к сети Интернет допускается применение ПО, входящего в Реестр разрешённого к использованию ПО.
При использовании сети Интернет необходимо:

- соблюдать требования настоящей Политики;
- использовать сеть Интернет исключительно для выполнения своих служебных обязанностей;
- ставить в известность отдел ИС СМТ о любых фактах нарушения требований настоящей Политики.

При использовании сети Интернет запрещено:

- использовать предоставленный Учреждением доступ в сеть Интернет в личных целях;
- использовать несанкционированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к сети Интернет;
- Совершать любые действия, направленные на нарушение нормального функционирования элементов ИС Учреждения;
- Публиковать, загружать и распространять материалы содержащие:
  - Конфиденциальную информацию, а также информацию, составляющую коммерческую тайну, за исключением случаев, когда это входит в должностные обязанности и способ передачи является безопасным, согласованным с отделом ИС СМТ;
  - угрожающую, клеветническую, непристойную информацию;
  - вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также ссылки на него;
  - фальсифицировать свой IP- адрес, а также прочую служебную информацию.

Учреждение оставляет за собой право блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены законодательством.

Блокирование и ограничение доступа пользователей к Интернет-ресурсам осуществляется на основе Регламента применения категорий Интернет-ресурсов.
Информация о посещаемых сотрудниками Учреждения Интернет-ресурсах протоколируется для последующего анализа и, при необходимости, может быть представлена Руководителям структурных подразделений, а также Руководству Учреждения для контроля.
Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО.

Шаблон 5

Политика использование мобильных устройств

Под использованием мобильных устройств (например, ноутбуков, планшетов и мобильных телефонов) и носителей информации в ИС Учреждения понимается их подключение к инфраструктуре ИС с целью обработки, приёма/передачи информации между ИС и мобильными устройствами, а также носителями информации.
На предоставленных Учреждением мобильных устройствах допускается использование ПО, входящего в Реестр разрешённого к использованию ПО.
К предоставленным Учреждением мобильным устройствам и носителям информации предъявляются те же требования ИБ, что и для стационарных АРМ. Целесообразность дополнительных мер обеспечения ИБ определяется отделом ИС СМТ.
При использовании предоставленных Учреждением мобильных устройств и носителей информации, сотрудник обязан:

- соблюдать требования настоящей Политики;
- использовать мобильные устройства и носители информации исключительно для выполнения своих служебных обязанностей;
- ставить в известность отдел ИС СМТ о любых фактах нарушения требований настоящей Политики;
- эксплуатировать и транспортировать мобильные устройства и носители информации в соответствии с требованиями производителей;
- обеспечивать физическую безопасность мобильных устройств и носителей информации всеми разумными способами;
- извещать отдел ИС СМТ о фактах утраты (кражи) мобильных устройств и носителей информации.

При использовании предоставленных сотрудника Учреждения мобильных устройств и носителей информации запрещено:

- использовать мобильные устройства и носители информации в личных целях;
- передавать мобильные устройства и носители информации другим лицам (за исключением администраторов ИС и ИБ);
- оставлять мобильные устройства и носители информации без присмотра, если не предприняты действия по обеспечению их физической безопасности.

Любое взаимодействие (обработка, приём\передача информации) инициированное сотрудником Учреждения между ИС и неучтёнными (личными) мобильным и устройствами, а также носителями информации, рассматривается как несанкционированное (за исключением случаев, оговорённых с администраторами ИС заранее). Учреждение оставляет за собой право блокировать или ограничивать использование таких устройств и носителей информации;
Информация об использовании сотрудниками Учреждения мобильных устройств и носителей информации в ИС протоколируется и, при необходимости, может быть представлена Руководителям структурных подразделений, а также руководству Учреждения.
Информация, хранящаяся на предоставляемых Учреждением мобильных устройствах и носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

В случае увольнения, предоставленные ему мобильные устройства и носители информации изымаются.

Перечень разрешенного программного обеспечения в мобильных устройствах определен в Приложении № 5 к настоящей Политике.

Шаблон 6

Политика защиты от вредоносного ПО

Отдел ИС СМТ регулярно проверяет сетевые ресурсы Учреждения антивирусным программным обеспечением и обеспечивает защиту входящей электронной почты от проникновения вирусов и другого вредоносного ПО.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление о системных ошибках, увеличение исходящего/входящего трафика и т.п.) сотрудник Учреждения должен незамедлительно оповестить об этом отдел ИС СМТ. После чего администратор ИБ должен провести внеочередную полную проверку на вирусы рабочей станции пользователя, проверив, в первую очередь, работоспособность антивирусного ПО.

В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения заражения своего руководителя и отдел ИС СМТ, а также владельца файла и смежные подразделения, использующие эти файлы в работе.
- Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.

Правила предупреждения вирусного заражения в ГИС «Бухгалтерия и кадры» определены в Инструкции пользователя по обеспечению безопасности информации при её обработке в ИС.

Шаблон 7

Политика управления установкой (инсталяцией) компонентов программного обеспечения

В ГИС «Бухгалтерия и кадры» разрешено использование только того программного обеспечения, его компонентов, утилит и драйверов, которые необходимы для обеспечения функционирования информационной системы, а также необходимы для выполнения служебных (должностных) обязанностей пользователями.

Установка программного обеспечения, его компонент, утилит и драйверов осуществляется только системными администраторами или администратором безопасности в соответствии с Приложением № 7. Пользователям запрещена установка любого ПО в ГИС «Бухгалтерия и кадры».

Пользователь имеет право подать заявку в виде служебной записки на включение в список разрешенного в ГИС программного обеспечения, необходимых ему для выполнения служебных (должностных) обязанностей программ, утилит, драйверов. В такой служебной записке обязательно указывается обоснование необходимости включения в этот список нового программного обеспечения. Срок рассмотрения заявки должен составлять не более 3 рабочих дней.

Администратор ежемесячно с помощью инструмента XSpider 7.8.24 проводит проверку соответствия состава программного обеспечения в ГИС «Бухгалтерия и кадры» списку разрешенного ПО. В случае выявления постороннего программного обеспечения, созывается группа реагирования на инциденты информационной безопасности, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

На серверной части ГИС «Бухгалтерия и кадры» при загрузке операционных систем серверов запускается следующее программное обеспечение:

- MS SQL Server;
- IIS;
- ...

На АРМ Пользователей ГИС «Бухгалтерия и кадры» при загрузке операционных систем серверов запускается следующее программное обеспечение:

- MS SQL Server;
- IIS;
- ...

На АРМ Администратора ГИС «Бухгалтерия и кадры» при загрузке операционных систем серверов запускается следующее программное обеспечение:

- MS SQL Server;
- IIS;
- ...

Шаблон 8

Политика обеспечения доверенной загрузки средств вычислительно техники

В {Название Организации} в качестве средства доверенной загрузки технических средств применяется {Название МДЗ}. {Убрать, если применяются компенсирующие меры}

Для работы с ресурсами ГИС «Бухгалтерия и кадры» выбираются такие технические средства, базовая система ввода-вывода которых (BIOS/UEFI) позволяет отключить возможность выбора источника загрузки в обход настроек BIOS/UEFI (вызов вариантов источников загрузки одной из функциональных клавиш).

Администратор контролирует работоспособность {Название МДЗ} в соответствии с планом периодических мероприятий по контролю защищенности информации. По результатам проверки делается запись в журнал периодического тестирования средств защиты информации. {Убрать, если применяются компенсирующие меры}

В случае некорректной работы средства доверенной загрузки на техническом средстве, такое техническое средство изымается из ГИС на время проведения ремонта/замены средства доверенной загрузки. В случае необходимости продолжения работы на техническом средстве, применяются следующие компенсирующие меры {Убрать, если применяются компенсирующие меры}:

- опечатываются USB-порты, входы для SD/Micro-SD и других карт памяти, CD/DVD/Blu-Ray-приводы и сами технические средства;
- устанавливается пароль администратора на вход в BIOS/UEFI и отключается возможность вызова источника загрузки нажатием функциональной клавиши (F1-F12) при загрузке;
- устанавливается усиленный визуальный контроль за техническим средством.

В проектной документации на систему защиты информации в ГИС «Бухгалтерия и кадры» обосновано применение компенсирующих мер, нейтрализующих угрозы безопасности информации, связанные с недоверенной загрузкой технических средств ГИС. {Убрать, если применяется МДЗ}

В качестве компенсирующей меры в ГИС «Бухгалтерия и кадры» применяется опечатывание USB-портов, входов для SD/Micro-SD и других карт памяти, CD/DVD/Blu-Ray-приводов и самих технических средств. Данная мера обеспечивает контроль доступа злоумышленника к интерфейсам ввода-вывода, позволяющим осуществить недоверенную загрузку. {Убрать, если применяется МДЗ}

В качестве компенсирующей меры в ГИС «Бухгалтерия и кадры» применяется установка пароля администратора на вход в BIOS/UEFI и отключение возможности вызова источника загрузки во время загрузки технического средства. Данная мера позволяет блокировать на программном уровне изменение источника загрузки при срыве пломбы с интерфейса ввода-вывода. {Убрать, если применяется МДЗ}

В качестве компенсирующей меры в ГИС «Бухгалтерия и кадры» применяется усиленный визуальный контроль за техническими средствами ГИС. Данная мера позволяет своевременно детектировать факты нарушения пломб технического средства, выявлять факты несанкционированного доступа и принимать меры реагирования. {Убрать, если применяется МДЗ}

Администратор контролирует выполнение компенсирующих мер в соответствии с планом периодических мероприятий по контролю защищенности информации. По результатам проверки делается запись в журнал периодического тестирования средств защиты информации. {Убрать, если применяется МДЗ}

Шаблон 9

Политика использования криптографического контроля

Все, поступающие в Учреждение, СКЗИ должны быть учтены в соответствующем журнале поэкземплярного учёта СКЗИ.

В Учреждении должно осуществляться управление ключами для эффективного применения криптографических методов. Компрометация или потеря криптографических ключей может привести к нарушению конфиденциальности, подлинности и/или целостности информации.

Все ключи должны быть защищены от изменения, утери и уничтожения. Кроме того, секретные и закрытые ключи должны быть защищены от несанкционированного раскрытия. Оборудование, используемое для генерации, хранения и архивирования ключей должно быть физически защищено.

Соглашения с внешними поставщиками криптографических услуг (например, удостоверяющими центрами) об уровне предоставляемого сервиса должны охватывать вопросы ответственности, надёжности сервиса и времени реакции при предоставлении сервиса.

Криптографические системы и методы следует использовать для защиты конфиденциальной информации, когда другие средства контроля не обеспечивают адекватной защиты.

Для критической информации должно использоваться шифрование при их хранении в базах данных или передаче по коммерческим или открытым сетям, таким как Интернет.

Шифрование любой другой информации в ИС Учреждения должно осуществляться только после получения письменного разрешения на это.

1. Требований по обеспечению ИБ при использовании шифрования

Шифрование – это криптографический метод, который может использоваться для обеспечения защиты конфиденциальной, важной или критичной информации.

СКЗИ должны поставляться разработчиками с полным комплектом эксплуатационной документации, включающей описание ключевой системы, правила работы с ней и обоснование необходимого организационно-штатного обеспечения.

Порядок применения СКЗИ определяется руководством Учреждения и должен включать:

- порядок ввода в действие, включая процедуры встраивания СКЗИ в ИС;
- порядок эксплуатации;
- порядок восстановления работоспособности в аварийных случаях;
- порядок внесения изменений;
- порядок снятия с эксплуатации;
- порядок управления ключевой информацией;
- порядок обращения с ключевой информацией, включая действия при смене и компрометации ключей.

Для шифрования конфиденциальной информации минимально допустимой длинной ключа является 128 бит.

При использовании шифрования в ИС Учреждения должны применяться только утверждённые стандартные алгоритмы и сертифицированные ФСБ России продукты, их реализующие.

2. Электронные цифровые подписи

ЭЦП обеспечивают защиту аутентификации и целостности электронных документов.

ЭЦП могут применяться для любой формы документа, обрабатываемого электронным способом. ЭЦП должны быть реализованы при использовании криптографического метода, основывающегося на однозначно связанной паре ключей, где один ключ используется для создания подписи (секретный/личный ключ), а другой – для проверки подписи (открытый ключ).

Необходимо с особой тщательностью обеспечивать конфиденциальность личного ключа, который следует хранить в секрете, так как любой, имеющий к нему доступ, может подписывать документы (платежи, контракты), тем самым фальсифицируя подпись владельца ключа. Защиты целостности открытого ключа должна обеспечиваться при использовании сертификата открытого ключа.

Криптографические ключи, используемые для цифровых подписей, должны отличаться от тех, которые используются для шифрования.

При использовании ЭЦП, необходимо учитывать требования действующего законодательства Российской Федерации, определяющего условия, при которых цифровая подпись имеет юридическую силу.

3. Управление ключами

Управление криптографическими ключами важно для эффективного использования криптографических средств.

Любая компрометация или потеря криптографических ключей может привести к компрометации конфиденциальности, подлинности и/или целостности информации. Следует применять систему защиты для обеспечения использования в ИС Учреждения криптографических методов в отношении открытых ключей, где каждый пользователь имеет пару ключей, открытый ключ (который может быть показан любому) и личный ключ (который должен храниться в секрете). Методы с открытыми ключами должны использоваться для шифрования и для генерации цифровых подписей.

Ключи необходимо защищать от изменения и разрушения, а секретным и личным ключам необходима защита от неавторизованного раскрытия. Криптографические методы могут также использоваться для этой цели. Физическую защиту следует применять для защиты оборудования, используемого для изготовления, хранения и архивирования ключей.

Сервер сертифицированного центра КУЦ должен хранить текущие открытые ключи для всех авторизованных на это сотрудников. Для безопасного взаимодействия с внешними пользователями ИС Учреждения необходимо использовать электронные сертификаты только из утверждённого списка сертифицированных центров.

Секретные ключи пользователей должны храниться так же, как и пароли. О любом подозрении на компрометацию секретного ключа пользователь должен немедленно доложить в отдел ИС СМТ.

Необходимо, чтобы система обеспечения безопасности использования ключей основывалась на согласовании способов, процедур и безопасных методов для:

- генерации ключей при использовании различных криптографических систем и приложений;
- генерации и получения сертификатов открытых ключей;
- рассылки ключей, предназначенных пользователям, включая инструкции по их активации при получении;
- хранения ключей (при этом необходимо наличие инструкции авторизованным пользователям для получения доступа к ключам);
- смены или обновления ключей, включая правила порядка и сроков смены ключей;
- порядка действий в отношении скомпрометированных ключей;
- аннулирования ключей, в том числе способы аннулирования или дезактивации ключей, если ключи были скомпрометированы или пользователь уволился из организации (в этом случае ключи необходимо архивировать);
- восстановление ключей, которые были утеряны или испорчены, для рассекречивания зашифрованной информации;
- архивирования и резервного копирования ключей;
- разрушения ключей;
- регистрация ключей и аудита действий, связанных с управлением ключами.

Для уменьшения вероятности компрометации, для ключей необходимо определить даты начала и конца действия, чтобы их можно было использовать лишь в течении ограниченного периода времени, который зависит от обстоятельств использования криптографических средств, контроля и от степени риска раскрытия информации.

Может потребоваться наличие процедур обработки юридических запросов, касающихся доступа к криптографическим ключам, например, чтобы зашифрованная информация стала доступной в незашифрованном виде для доказательств в суде.

Необходимо обеспечивать защиту открытых ключей от угроз подделывания цифровой подписи и замены открытого ключа пользователя своим. Эта проблема решается с помощью сертификата открытых ключей. Сертификаты необходимо изготавливать таким способом, который однозначно связывал бы информацию, относящуюся к владельцу пары

открытого/секретного ключей, с открытым ключом. Поэтом важно, чтобы процессу управления, в рамках которого формируются эти сертификаты, можно было доверять.

Соглашения с внешними поставщиками криптографических услуг (например, с удостоверяющими центрами) об уровне предоставляемого сервиса должны охватывать вопросы ответственности, надёжности сервиса и времени реакции при предоставлении сервиса.

Шаблон 10

Политика резервного копирования

Резервирование информационных ресурсов (программного обеспечения, баз данных, средств защиты информации) ГИС «Бухгалтерия и кадры» осуществляется в соответствии с инструкцией администратора безопасности информации и в соответствии с Приложением № 10 к настоящей Политике.

Администратор осуществляет с периодичностью, установленной в плане мероприятий по обеспечению режима защиты информации проверку работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий. По результатам проверки делается запись в журнале учета мероприятий по контролю за соблюдением режима защиты информации. В случае выявления проблем с системой резервирования, принимаются меры по восстановлению ее работоспособности. После восстановления работоспособности системы резервирования осуществляется внеплановое резервное копирование всех информационных ресурсов ГИС «Бухгалтерия и кадры».

Резервирование технических средств осуществляется в соответствии с проектной документацией (эскизным проектом) на систему защиты информации ГИС «Бухгалтерия и кадры».

Восстановление из резервных копий является основным методом восстановления работоспособности информационной системы после ликвидации нештатных ситуаций.

Нештатными ситуациями являются:

- разглашение информации ограниченного доступа сотрудниками {Название Организации}, имеющими к ней право доступа, в том числе:
    - разглашение информации лицам, не имеющим права доступа к защищаемой информации;
    - передача информации по незащищенным каналам связи;
    - обработка информации на незащищенных технических средствах обработки информации;
    - опубликование информации в открытой печати и других средствах массовой информации;
    - передача носителя информации лицу, не имеющему права доступа к ней;
    - утрата носителя с информацией.
- неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:
    - несанкционированное изменение информации;
    - несанкционированное копирование информации;
- несанкционированный доступ к защищаемой информации:
    - несанкционированное подключение технических средств к средствам и системам ГИС «Бухгалтерия и кадры»;
    - использование закладочных устройств;

    - использование злоумышленником легальных учетных записей пользователей для доступа к информационным ресурсам ГИС «Бухгалтерия и кадры»;
    - использование злоумышленником уязвимостей программного обеспечения ГИС;
    - использование злоумышленником программных закладок;
    - заражение ГИС злоумышленником программными вирусами;
    - хищение носителей информации;
    - нарушение функционирования технических средств обработки информации;
    - блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;
- дефекты, сбои, отказы, аварии технических средств и систем ГИС;
- дефекты, сбои, отказы программного обеспечения ГИС;
- сбои, отказы и аварии систем обеспечения ГИС;
- природные явления, стихийные бедствия:
    - термические, климатические факторы (аномально низкие или аномально высокие температуры воздуха, пожары, наводнения, снегопады и т. д.);
    - механические факторы (повреждения зданий, землетрясения и т. д.);
    - электромагнитные факторы (отключение электропитания, скачки напряжения, удары молний и т. д.).

В случае возникновения нештатной ситуации, порядок действий при которой не регламентирован настоящей Политикой, Администратором, Ответственным и ГРИИБ вырабатывается конкретный план действий с учетом текущей ситуации.

Порядок оповещения должностных лиц и сроки выполнения мероприятий при нештатных ситуациях определены в Приложении № 11 настоящей Политики.

С целью усовершенствования координации действий должностных лиц по реагированию на нештатные ситуации должны проводиться регулярные тренировки по различным видам нештатных ситуаций. В случае выявления по результатам тренировок изъянов в положениях настоящей Политики, касающихся реагирования на нештатные ситуации, в нее могут вноситься изменения.

Инциденты безопасности информации также являются нештатной ситуацией. При выявлении нештатных ситуаций, повлекших нарушение целостности, доступности или конфиденциальности защищаемой информации по вине внутреннего или внешнего нарушителя, созывается ГРИИБ, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем предпринимаются следующие действия:

- корректное отключение технических средств ГИС до истощения ресурса источников бесперебойного питания, перегрева технических средств и до наступления других негативных последствий;
- предпринимаются меры по устранению причин, вызвавших сбои, отказы и аварии средств и систем ГИС а также меры по замене/ремонту вышедших из строя средств и систем;
- в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации, Администратор восстанавливает их из резервных копий.

В случае нештатных ситуаций, связанных со стихийными бедствиями и деструктивными природными явлениями выполняются следующие действия:

- Пользователи корректно отключают и обесточивают свои рабочие места;
- системные администраторы корректно отключают и обесточивают серверы и сетевое оборудование;
- Администратор предпринимает меры к эвакуации носителей информации и носителей резервных копий;
- в случае нарушения корректной работы технических средств в ГИС в результате стихийных бедствий или природных явлений принимаются меры по ремонту/замене вышедшего из строя оборудования;
- в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации в результате стихийных бедствий или природных явлений, Администратор восстанавливает их из резервных копий;
- в случае стихийных действий/природных явлений, опасных для жизни человека в первую очередь организуется эвакуация сотрудников и только по возможности организуется эвакуация технических средств, носителей информации и носителей с резервными копиями.

Шаблон 11

Политика контроля состава технических средств, программного обеспечения и средств защиты информации

Состав технических средств (далее – ТС), программного обеспечения (далее – ПО) и средств защиты информации (далее – СрЗИ) ГИС «Бухгалтерия и кадры» фиксируется в техническом паспорте на информационную систему. Технический паспорт является эталоном состава ТС, ПО и СрЗИ, по которому осуществляется периодический контроль.

В случае добавления новых ТС, ПО и СрЗИ в состав ГИС «Бухгалтерия и кадры» или удаления существующих компонентов, на основании акта ввода в эксплуатацию (или акта вывода из эксплуатации) максимально оперативно вносятся изменения в Технический паспорт.

Администратор осуществляет контроль состава ТС, ПО и СрЗИ не реже одного раза в месяц.

Выявление несоответствия состава ТС, ПО и СрЗИ техническому паспорту ГИС «Бухгалтерия и кадры» является инцидентом безопасности. В случае выявления фактов несоответствия Администратор устанавливает причины самостоятельно или созывает ГРИИБ.

В случае выявления несоответствия состава ТС, ПО и СрЗИ, Администратор принимает меры по оперативному исключению (восстановлению) из состава (в составе) информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

Администратор осуществляет контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принимает меры, направленные на устранение выявленных недостатков. В случае, если сертификат соответствия истек, но был продлен производителем СрЗИ, Администратор запрашивает актуальную заверенную копию сертификата. В случае, если сертификат соответствия истек, но не был продлен производителем СрЗИ, то Администратор сообщает об этом руководителю {Название Организации}, который принимает решение об организации самостоятельной сертификации использующегося СрЗИ, либо об обновлении использующегося СрЗИ до актуальной версии, либо о замене использующегося СрЗИ на другое аналогичное сертифицированное СрЗИ.

Шаблон 12

Политика дистанционной работы

1. Ответственность

Ответственность за установку, настройку и администрирование средств обработки информации на рабочем месте пользователя возлагается на службу информационных технологий или иную службу {Название Организации}.

Ответственность за соблюдение правил или политики организации рабочего места возлагается на всех работников фирмы и третьих лиц, использующих средства обработки информации.

Контроль выполнения политики организации рабочего места возлагается на службу информационной безопасности {Название Организации}.

Провести анализ

2. Назначение и область действия

Настоящая политика устанавливается для эффективной организации дистанционной работы пользователей в целях:

- Защиты сетевых сервисов;
- Предотвращения неавторизованного доступа к операционным системам;
- Обеспечение информационной безопасности при работе в дистанционном режиме.

Правила распространяются на всех работников фирмы и третьих лиц, участвующих в организации работы и работающих в дистанционном режиме, и являются обязательными для исполнения.

Все исключения из настоящих правил должны быть согласованы со службой информационной безопасности {Название Организации}..

3. Основные требования

Предоставление пользователю дистанционного доступа должно быть согласовано с руководителем подразделения данного сотрудника и владельцем информационных ресурсов, к которым предоставляется доступ. Управление дистанционным доступом осуществляется в соответствии с установленными процедурами.

Для контроля доступа пользователя в дистанционном режиме должны использоваться надежные методы аутентификации, включая:

- обратный вызов;
- аутентификацию узла по физическому адресу;
- решения для VPN;
- выделенные физические линии и т.д.

При использовании обратного вызова должна быть блокирована возможность переадресации

Доступ в дистанционном режиме обязательно организуется с использованием установленных средств шифрования траффика.

Дистанционный доступ к используемым диагностическим и конфигурационным портам оборудования должен регистрироваться. Возможность дистанционного доступа к неиспользуемым диагностическим или конфигурационным портам оборудования должна быть исключена.

Для сеансов дистанционного доступа должно быть установлено время бездействия, во время которого оборудование отключается, и сеанс работы прекращается.

Для критических приложений должно использоваться ограничение времени соединения дистанционного доступа.

Обязательными условиями предоставления дистанционного доступа к информационным ресурсам фирмы являются:

- Установка и своевременное обновление на компьютере пользователя средств антивирусной защиты.
- Установка и надлежащая настройка на компьютере пользователя применяемых в фирме или организации средств предотвращения атак.

Настройка локальных параметров безопасности на компьютере пользователя в соответствии с применяемыми в компании групповыми политиками безопасности.

4. Ответственность
Ответственность за организацию работы в дистанционном режиме возлагается на службу информационных технологий {Название Организации}.

Ответственность за соблюдение правил возлагается на всех сотрудников фирмы и третьих лиц, работающих в дистанционном режиме. Контроль выполнения и пересмотр политики возлагается на службу безопасности информации. Провести анализ

Шаблон 13

Политика использования сетевых служб

Политика сетевой безопасности в {Название Организации} представляет совокупность положений, правил и практических приемов, устанавливающих подход организации к использованию ее сетевых ресурсов и определяющих, как следует обеспечивать защиту ее сетевой инфраструктуры и сервисов.
Политика сетевой безопасности {Название Организации} включает:

- политику доступа к сетевым сервисам;
- политику реализации межсетевых экранов.

Политика доступа к сетевым сервисам определяет список сервисов Интернет, к которым пользователи должны иметь ограниченный доступ. Под сервисами Интернет будем понимать сервисы, предоставляемые в сети Интернет пользователям, программам, системам, уровням, функциональным блокам. Наиболее распространенными сервисами являются хранение данных, передача сообщений и блоков данных, электронная и речевая почта, предоставление соединений, видеосервис.
Необходимо ограничение методов доступа, чтобы пользователи не могли обращаться к «запрещенным» сервисам Интернет обходными путями. Набор обходных путей зависит от политики безопасности для данного межсетевого экрана.

Политика реализации межсетевых экранов определяет правила доступа к ресурсам внутренней сети. Правила доступа к внутренним ресурсам должны базироваться на одном из следующих принципов:

- запрещать все, что не разрешено в явной форме;
- разрешать все, что не запрещено в явной форме.

Реализация межсетевого экрана на основе обоих принципов.

Шаблон 14

Политика по работе с инцидентами информационной безопасности
Политика разработана в целях выявления, предотвращения и устранения последствий нарушений законодательства Российской Федерации в области обработки конфиденциальной информации.

1. Инциденты в области информационной безопасности возникают при нарушении правил и требований информационной безопасности.
В ходе инцидента реализуются (или создается возможность для реализации) угрозы информационной безопасности, что, как правило, приводит к нанесению вреда активам {название организации}.
Работа с инцидентами в области информационной безопасности помогает определить наиболее актуальные угрозы информационной безопасности и создает обратную связь в системе обеспечения информационной безопасности, что способствует повышению общего уровня защиты информационных ресурсов информационных систем персональных данных.

Работа с инцидентами включает в себя 3 направления:

- выявление инцидентов в области информационной безопасности;
- реакция на инциденты в области информационной безопасности;
- предупреждение инцидентов в области информационной безопасности.

2. Выявление инцидентов в области информационной безопасности

Работа по выявлению инцидентов в области информационной безопасности включает в себя мероприятия, направленные на:

- выявление инцидентов в области информационной безопасности с помощью технических средств;
- выявление инцидентов в области информационной безопасности в ходе мероприятий по контролю за обработкой персональных данных;
- выявление инцидентов с помощью персонала {название организации}.

3. Реакция на инциденты в области информационной безопасности

Реакция на инциденты в области информационной безопасности включает в себя:

- фиксацию инцидента в области информационной безопасности;
- определение границ инцидента и ущерба (в том числе потенциального) от реализации угроз информационной безопасности в ходе инцидента;
- ликвидация последствий инцидента и полное либо частичное возмещение ущерба;
- наказание виновных в инциденте информационной безопасности.

4. Предупреждение инцидентов в области информационной безопасности

Предупреждение инцидентов строится на:

- планомерной деятельности по повышению уровня осознания информационной безопасности руководством и сотрудниками {название организации};
- проведения мероприятий по обучению сотрудников {название организации} правилам и способам работы со средствами защиты информационных систем персональных данных;
- доведении до сотрудников норм законодательства в области защиты персональных данных и внутренних документов {название организации}, устанавливающих ответственность за нарушение требований информационной безопасности;
- разъяснительной работе с увольняющимися сотрудниками и сотрудниками, принимающимися на работу;
- своевременной модернизации системы обеспечения информационной безопасности информационных систем персональных данных с учетом возникновения новых угроз информационной безопасности;
- своевременном обновлении программного обеспечения, в т. ч. баз сигнатур антивирусных средств.

5. Причины инцидентов в области информационной безопасности

Причинами инцидентов в области информационной безопасности являются:

- действие враждебных интересам {название организации} организаций и отдельных лиц;
- отсутствие персональной ответственности за обеспечение информационной безопасности персональных данных сотрудников {название организации} их руководителей;
- недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности персональных данных;
- отсутствие моральной и материальной стимуляции за соблюдение правил и требований информационной безопасности;

- недостаточная техническая оснащённость подразделений, ответственных за обеспечение информационной безопасности;
- совмещение функций по разработке и сопровождению или сопровождению и контролю за информационными системами;
- наличие привилегированных бесконтрольных пользователей в информационной системе;
- пренебрежение правилами и требованиями информационной безопасности сотрудниками {название организации};
- и другие причины.

6. Расследование инцидентов в области информационной безопасности

Расследование инцидентов в области информационной безопасности должно включать в себя:

- формирование комиссии по расследованию инцидента в области информационной безопасности;
- определение границ инцидента – информационных ресурсов, технических средств и персонала, затронутых инцидентом;
- определение причин инцидента, факторов, влияющих на возникновение инцидента;
- определение участников инцидента;
- определение последствий инцидента;
- составление заключения по результатам расследования;
- выработка рекомендаций по предотвращению возникновения подобных инцидентов в будущем.

7. Работа с персоналом по предупреждению инцидентов

Как правило, самым слабым звеном в любой системе безопасности является человек. Наличие современных доступных способов воздействия на персонал {название организации}, таких как социальная инженерия, фишинг, подмена электронных идентификаторов, номеров телефонов и т. д., делает пользователя информационной системы персональных данных частым объектом внимания злоумышленника. Поэтому направление работы с персоналом является основным направлением работы подразделений информационной безопасности.

В работе с персоналом основной упор должен делаться не на наказание сотрудника за нарушения в области информационной безопасности, а на поощрение за надлежащие выполнение требований информационной безопасности, проявление личной инициативы в укреплении системы информационной безопасности.

Персонал {название организации} является так же важным источником сведений об инцидентах информационной безопасности. Поэтому необходимо донести до сотрудников информацию о том, что оперативно предоставленные сведения об инциденте информационной безопасности являются поводом для смягчения либо отмены наказания за нарушение требований информационной безопасности.

Частой причиной инцидентов информационной безопасности является личная обида подчиненных на своих руководителей, либо коллег. Поэтому благоприятный микроклимат в коллективе является необходимым фактором обеспечения информационной безопасности в организации.

Шаблон 15

Политика обеспечения непрерывности ИТ-сервисов

Настоящая политика устанавливает принципы менеджмента непрерывности ИТ-сервисов в {название организации}. Процесс Управления Непрерывностью ИТ-сервисов входит в общий Процесс Менеджмента Непрерывностью Бизнеса (МНБ).

Политика МНБ определяет следующие процессы:

- организационную деятельность по установлению способности к непрерывности бизнеса;
- непрерывный менеджмент и поддержку способности к обеспечению непрерывности бизнеса.

1. Организационная деятельность включает в себя установление требований и полного цикла непрерывности бизнеса от проектирования, построения, внедрения до первоначального применения проверки способности организации к непрерывности бизнеса.

2. Непрерывная поддержка и менеджмент включают в себя: внедрение непрерывности бизнеса в организации; проведение регулярных учений по применению планов обеспечения непрерывности бизнеса; актуализацию и обмен информацией в соответствии с этим планом, особенно, если происходят существенные изменения в производственных площадях, персонале, организационной структуре, производственных и технологических процессах или рыночных условиях.

3. Цели применения

Политика в области МНБ должна соответствовать природе, масштабу, сложности, географии и критичности видов деятельности организации, отражать ее культуру, взаимосвязанные области и деловую среду. Политика в области МНБ определяет требования к процессу обеспечения непрерывности бизнеса и должна обеспечивать соответствие действий в области непрерывности бизнеса потребностям организации в случае возникновения инцидента, а также развитие способности организации к непрерывности бизнеса. Способность к МНБ должна быть интегрирована в деятельность организации по управлению изменениями таким образом, чтобы способность к непрерывности бизнеса способствовала росту номенклатуры продукции и объема услуг.

4. Основные положения политики непрерывности бизнеса

Политика в области непрерывности бизнеса должна обеспечивать организации документированные принципы и цели, к которым должна стремиться организация и, на соответствие которым, необходимо проводить измерение способности к непрерывности бизнеса. Политика в области МНБ утверждается руководителем организации {название организации}, например, генеральным директором или председателем совета директоров.

В области МНБ организацией {название организации} определены:

- области применения МНБ в организации;
- необходимые ресурсы для МНБ;
- принципы, руководящие указания и минимальное количество стандартов организации в области МНБ;

- ссылки на соответствующие стандарты, инструкции или другие нормативные акты организации, которые должны быть включены в документы или могут быть использованы как точки отсчета.

Организация {название организации} должна поддерживать в рабочем состоянии политику, стратегии, планы и решения в области МНБ и проводить их анализ через запланированные интервалы времени в соответствии с потребностями организации.

5. Распределение ответственности и полномочий

Высшее руководство организации {название организации} должно назначить:

- лицо из числа высшего руководства, наделенное соответствующими полномочиями, ответственное за политику в области МНБ и ее внедрение;
- одного или несколько лиц, ответственных за выполнение и поддержку программы МНБ.

Обязанности, подотчетность, ответственность и полномочия персонала должны быть установлены в рабочих и должностных инструкциях.

Анализ этих обязанностей необходимо проводить в процессе аудита организации.

Надлежащее выполнение обязанностей в области обеспечения непрерывности бизнеса может быть усилено путем их включения в политику организации в области аттестации, компетентности и поощрения персонала.

6. Осуществление непрерывности бизнеса в организации

Деятельность по выполнению программы непрерывности бизнеса должна включать в себя проектирование, разработку и внедрение программы.

Организация должна осуществлять следующие действия:

- обмен информацией о программе с причастными сторонами;
- организацию и/или обеспечение соответствующего обучения персонала;
- проведение учений по обеспечению непрерывности бизнеса (см. раздел 9).

5.3.2 Организация может адаптировать признанные методы менеджмента для обеспечения эффективного управления программой непрерывности бизнеса.

13. Порядок действий сотрудников (персонала) банка и перечень мероприятий, которые должны быть выполнены в момент и после возникновения нестандартных и чрезвычайных ситуаций

Порядок действий сотрудников (персонала) головного офиса банка и перечень мероприятий, которые должны быть выполнены в момент и после возникновения нестандартных и чрезвычайных ситуаций, определён приложениями к настоящей политике с учётом особенности и причин возникновения нестандартных и чрезвычайных ситуаций.

Шаблон 16

Политика обеспечения восстановления

В Учреждении должны быть разработаны и реализованы планы, которые позволят продолжить или восстановить операции и обеспечить требуемый уровень доступности информации в установленные сроки после прерывания или сбоя критически важных бизнес-процессов.

В каждом плане поддержки непрерывности бизнеса должны быть чётко указаны условия начала его исполнения и сотрудники, ответственные за выполнение каждого фрагмента плана. При появлении новых требований необходимо внести поправки в принятые планы действия в нештатных ситуациях.
Для каждого плана должен быть назначен определённый владелец. Правила действия в нештатных ситуациях, планы ручного аварийного восстановления и планы возобновления деятельности должны находиться в ведении владельцев соответствующих ресурсов или процессов, к которым они имеют отношение.

План восстановления определён приложением к настоящей политике.

Шаблон 17

Предоставление услуг сторонним организациям

1. Соглашения о предоставлении услуг.
В соглашения о предоставлении услуг {Название Организации} сторонним организациям должны быть включены требования безопасности, описание, объёмы и характеристики качества предоставляемых услуг.

2. Анализ предоставления услуг
Услуги, отчёты и записи, предоставляемые {Название Организации} сторонним организациям, должны постоянно проверяться и анализироваться. В отношениях со сторонней организацией должны присутствовать следующие процессы:

- контроль объёма и качества услуг, оговоренных в соглашениях;
- предоставление сторонней организации информации об инцидентах ИБ, связанных с предоставляемыми услугами, и совместное изучение этой информации;
- анализ предоставленных сторонними организациями отчётов о предоставленных услугах;
- управление любыми обнаруженными проблемами.

3. Приёмка систем
В {Название Организации} должен быть разработан и утверждён порядок приёмки новых ИС, обновления и новых версий ПО.

ПРИЛОЖЕНИЕ Е

Оформлене акта классификации информационных систем.

Утверждаю
Руководитель предприятия
"____"_____"____"г.

АКТ

классификации информационной системы обработки информации

_____XXXXXXXXXXXXXXXX_____

(наименование информационной системы)

Комиссия, в соответствии с приказом от "____"_____"____"г.	N____	в составе:
председатель: Xxxxxxxxxxxxx X.X.		
члены комиссии: Xxxxxxxxxxxxx X.X. Xxxxxxxxxxxxx X.X. Xxxxxxxxxxxxx X.X.		

провела классификацию информационной системы

_____XXXXXXXXXXXXXXXX_____,

(наименование информационной системы)

рассмотрев исходные данные на автоматизированную систему обработки информации (АС) наименование автоматизированной системы условия ее эксплуатации (многопользовательский, однопользовательский; с равными или разными правами доступа к информации {выбрать нужное}), с учетом характера обрабатываемой информации (служебная тайна, коммерческая тайна, персональные данные и т.д. {выбрать нужное}) и в соответствии с руководящими документами Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации,

РЕШИЛА:

Установить АС *наименование автоматизированной системы*

класс _XX_.

Председатель _____ Xxxxxxxxxxxxx X.X.

Члены комиссии _____ Xxxxxxxxxxxxx X.X.

_____ Xxxxxxxxxxxxx X.X.

_____ Xxxxxxxxxxxxx X.X.

ПРИЛОЖЕНИЕ Ж

Условные обозначения к планировкам выделенных помещений

Обозначение	Наименование
	Граница контролируемой зоны

Таблица. Характеристики конструкций

№ варианта	Стены	Дверь	Окно
1	Стена из кирпичной кладки без штукатурки (из красного кирпича): в 1,5 кирпича	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 4,5 см: без уплотняющих прокладок	Одинарное остекление без уплотнительных прокладок, толщина 3,0 мм
2	Стена из кирпичной кладки без штукатурки (из красного кирпича): в 2 кирпича	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 4,5 см: с уплотняющими прокладками	Одинарное остекление без уплотнительных прокладок, толщина 4,0 мм
3	Стена из кирпичной кладки без штукатурки (из красного кирпича): в 2,5 кирпича	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 2,5 см из 3 мм фанеры без уплотняющих прокладок	Одинарное остекление без уплотнительных прокладок, толщина 6,0 мм
4	Стена из кирпичной кладки без штукатурки (из красного кирпича): в 2 кирпича	-	Двойное остекление, расстояние между стеклами 57 мм, без звукопоглощающего материала, толщина 3,0/3,0
5	Стена из пустотелого кирпича, толщина 380,0 мм	-	Двойное остекление, расстояние между стеклами 57 мм, со звукопоглощающим материалом, толщина 3,0/3,0
6	Стена из пустотелого кирпича, толщина 510,0 мм	Глухая щитовая дверь, толщиной 40 мм, облицованная с двух сторон фанерой, толщиной 4 мм: С уплотняющими прокладками	Двойное остекление, расстояние между стеклами 90 мм, без звукопоглощающего материала, толщина 3,0/3,0
7	Стена из железобетона, толщина 160,0 мм	Щитовая дверь из твердых древесноволокнистых плит толщиной 4-6 мм с воздушным зазором 50 мм, заполненным	-

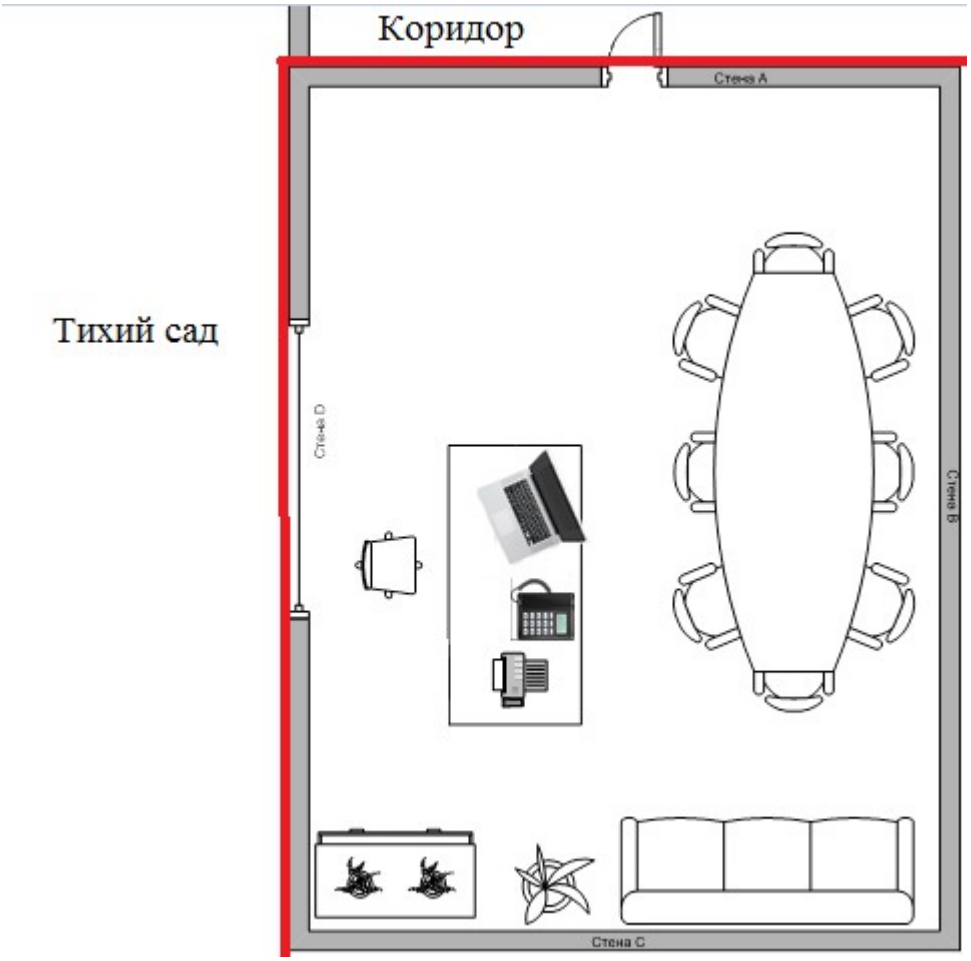
		стекловатой: Без уплотняющих прокладок	

8	Стена из железобетона, толщина 180,0 мм	Щитовая дверь из твердых древесноволокнистых плит толщиной 4-6 мм с воздушным зазором 50 мм, заполненным стекловатой: С уплотняющими прокладками	Двойное остекление, расстояние между стеклами 57 мм, без звукопоглощающего материала, толщина 4,0/4,0
9	Стена из железобетона, толщина 160,0 мм	-	Двойное остекление, расстояние между стеклами 57 мм, со звукопоглощающим материалом, толщина 4,0/4,0
10	Стена из железобетона, толщина 200,0 мм	-	Двойное остекление, расстояние между стеклами 90 мм, без звукопоглощающего материала, толщина 4,0/4,0
11	Стена из железобетона, толщина 300,0 мм	-	Двойное остекление, расстояние между стеклами 57 мм, без звукопоглощающего материала, толщина 6,0/3,0
12	Стена из железобетона, толщина 800,0 мм	-	Двойное остекление, расстояние между стеклами 90 мм, без звукопоглощающего материала, толщина 6,0/3,0
13	Газобетонная плита, толщина 240,0 мм	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 4,5 см: без уплотняющих прокладок	-
14	Газобетонная плита, толщина 240,0 мм	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 4,5 см: с уплотняющими прокладками	Двойное остекление, расстояние между стеклами 190 мм, без звукопоглощающего материала, толщина 6,0/6,0

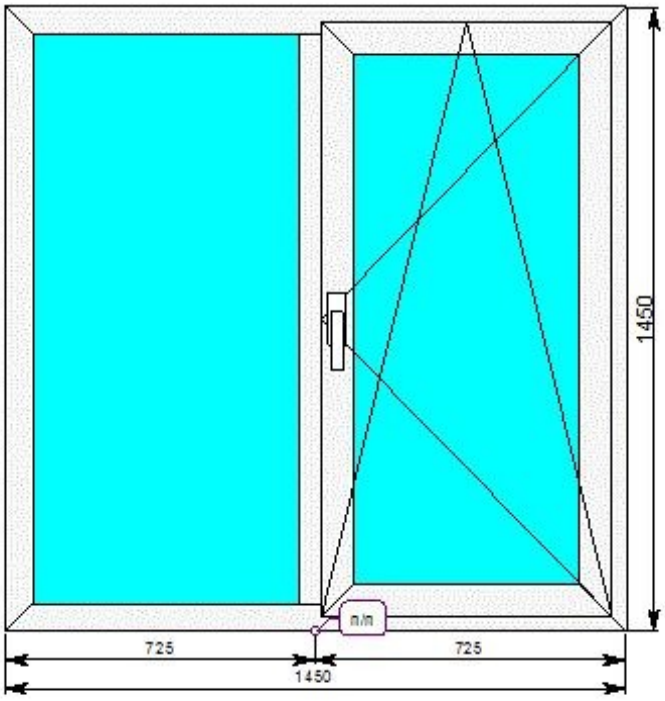
15	Керамзитобетонная плита, толщина 100,0 мм	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 2,5 см из 3 мм фанеры без уплотняющих прокладок	-
16	Керамзитобетонная плита, толщина 120,0 мм	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 2,5 см из 3 мм фанеры без уплотняющих прокладок, оклеенная фанерой размером 90х200 см без уплотняющих прокладок	Одинарное остекление без уплотнительных прокладок, толщина 3,0 мм
17	Шлакоблоки, отштукатуренные с двух сторон, толщина 220,0 мм	Глухая щитовая дверь, толщиной 40 мм, облицованная с двух сторон фанерой, толщиной 4 мм: Без уплотняющих прокладок	Одинарное остекление без уплотнительных прокладок, толщина 4,0 мм
18	Стена из пемзобетона, толщина 140,0 мм	-	Одинарное остекление без уплотнительных прокладок, толщина 6,0 мм
19	Стена из пемзобетона, толщина 140,0 мм	Щитовая дверь из твердых древесноволокнистых плит толщиной 4-6 мм с воздушным зазором 50 мм, заполненным стекловатой: Без уплотняющих прокладок	Двойное остекление, расстояние между стеклами 57 мм, без звукопоглощающего материала, толщина 3,0/3,0
20	Стена из пемзобетона, толщина 140,0 мм	Щитовая дверь из твердых древесноволокнистых плит толщиной 4-6 мм с воздушным зазором 50 мм, заполненным стекловатой: С уплотняющими прокладками	Одинарное остекление без уплотнительных прокладок, толщина 3,0 мм

Варианты планировок выделенных помещений

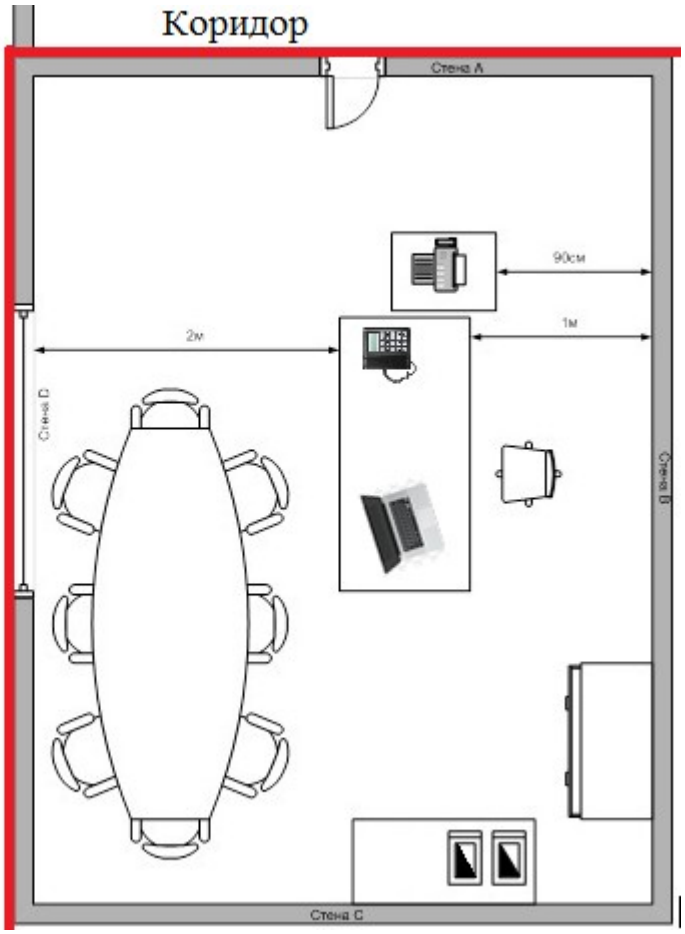
1. Помещение для переговоров №1



Размеры помещ.: 4х6м, h=3м.
Размер двери: 2х0,9м.

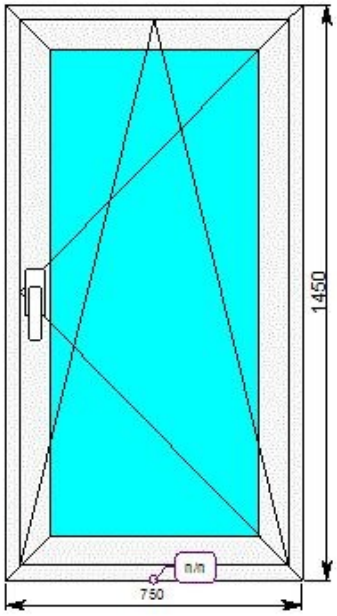


2. Помещение для переговоров №2

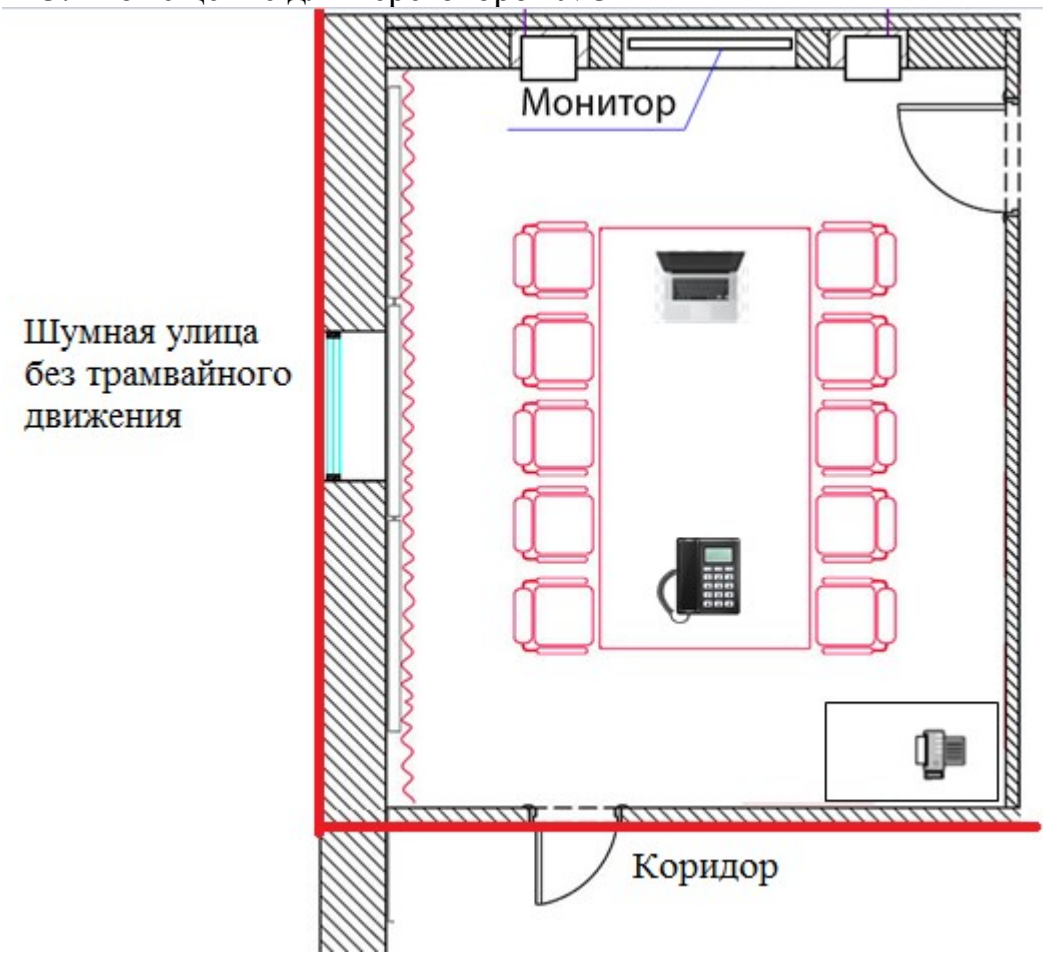


Тихая улица

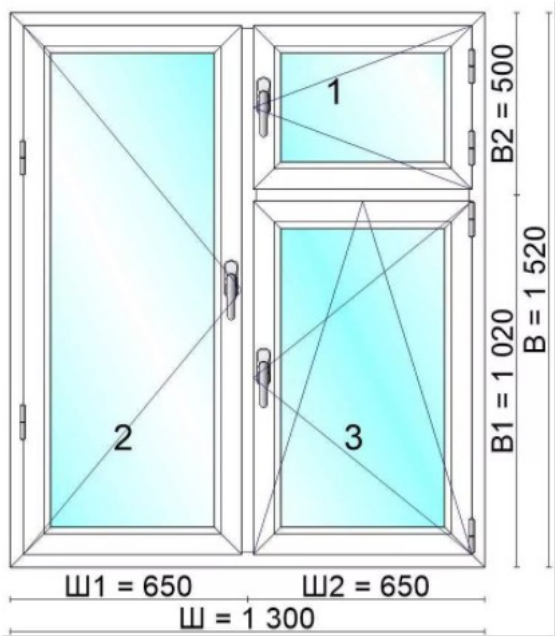
Размеры: 4,5х6м, h=3,5м.
Размер двери: 2х0,9м.



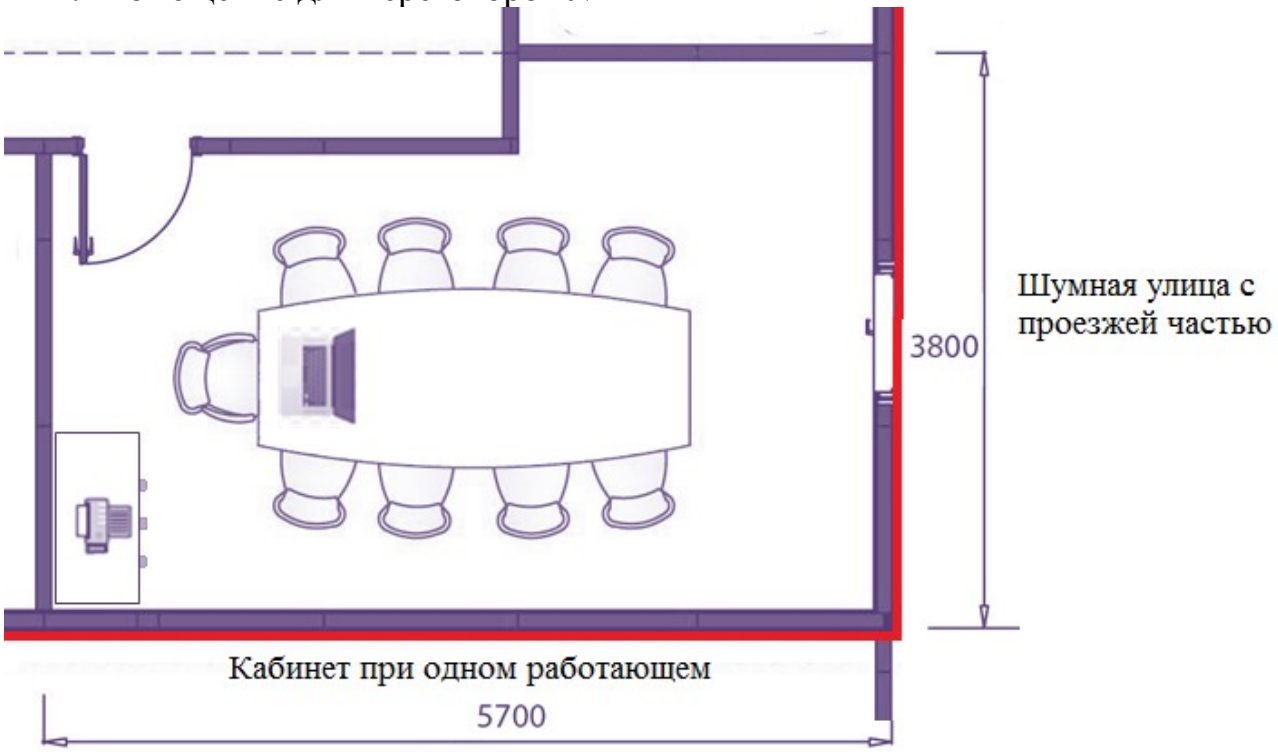
3. Помещение для переговоров №3



Размеры: 4,5х6м, h=3м.
Размер двери: 2х0,9м.

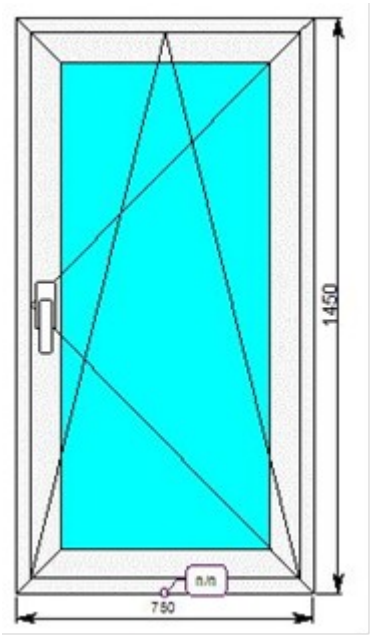


4. Помещение для переговоров №4

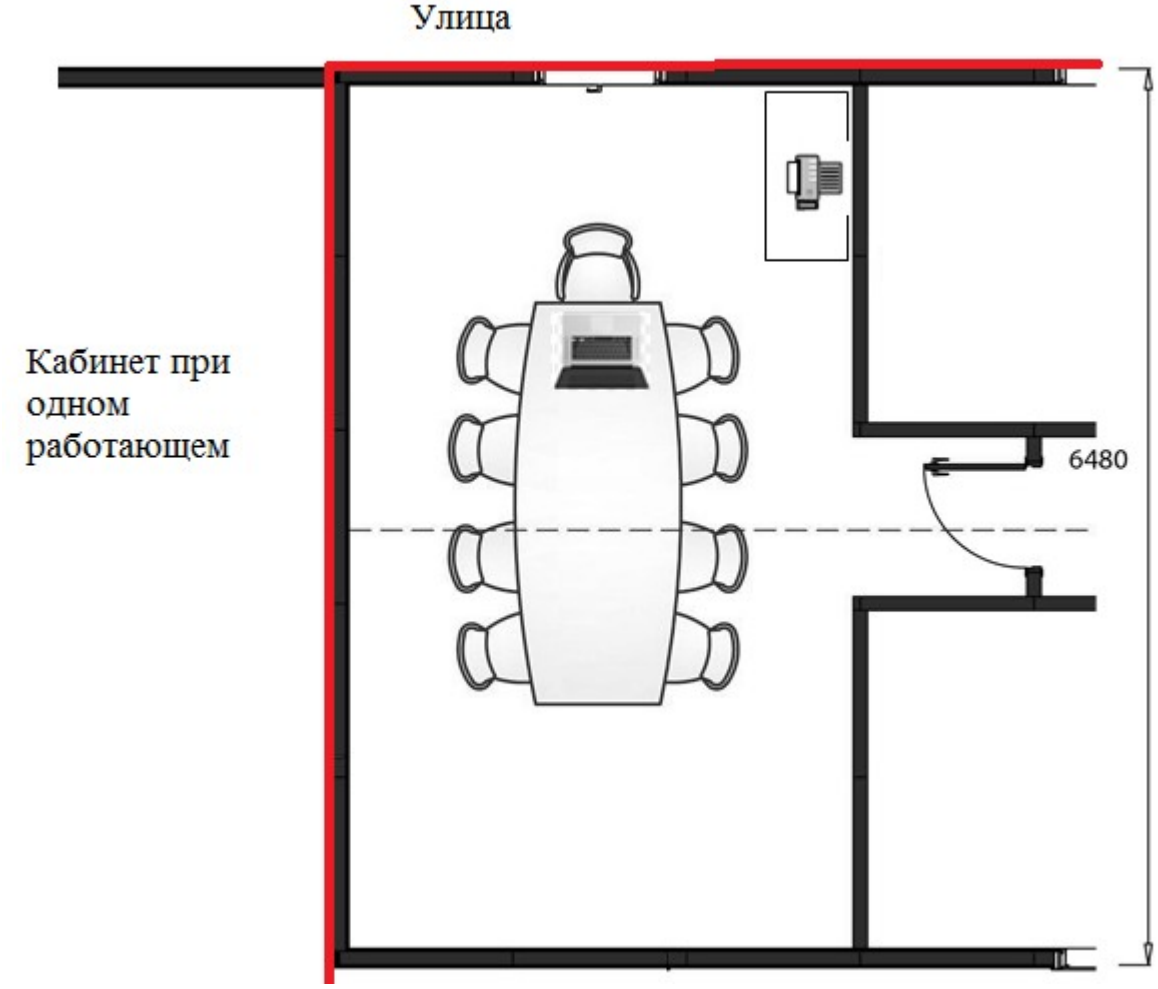


h=3м

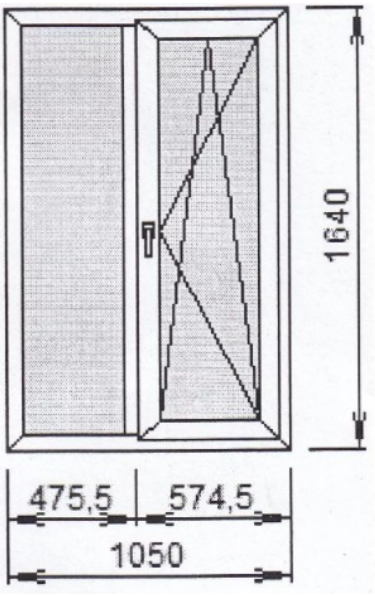
Размер окна:



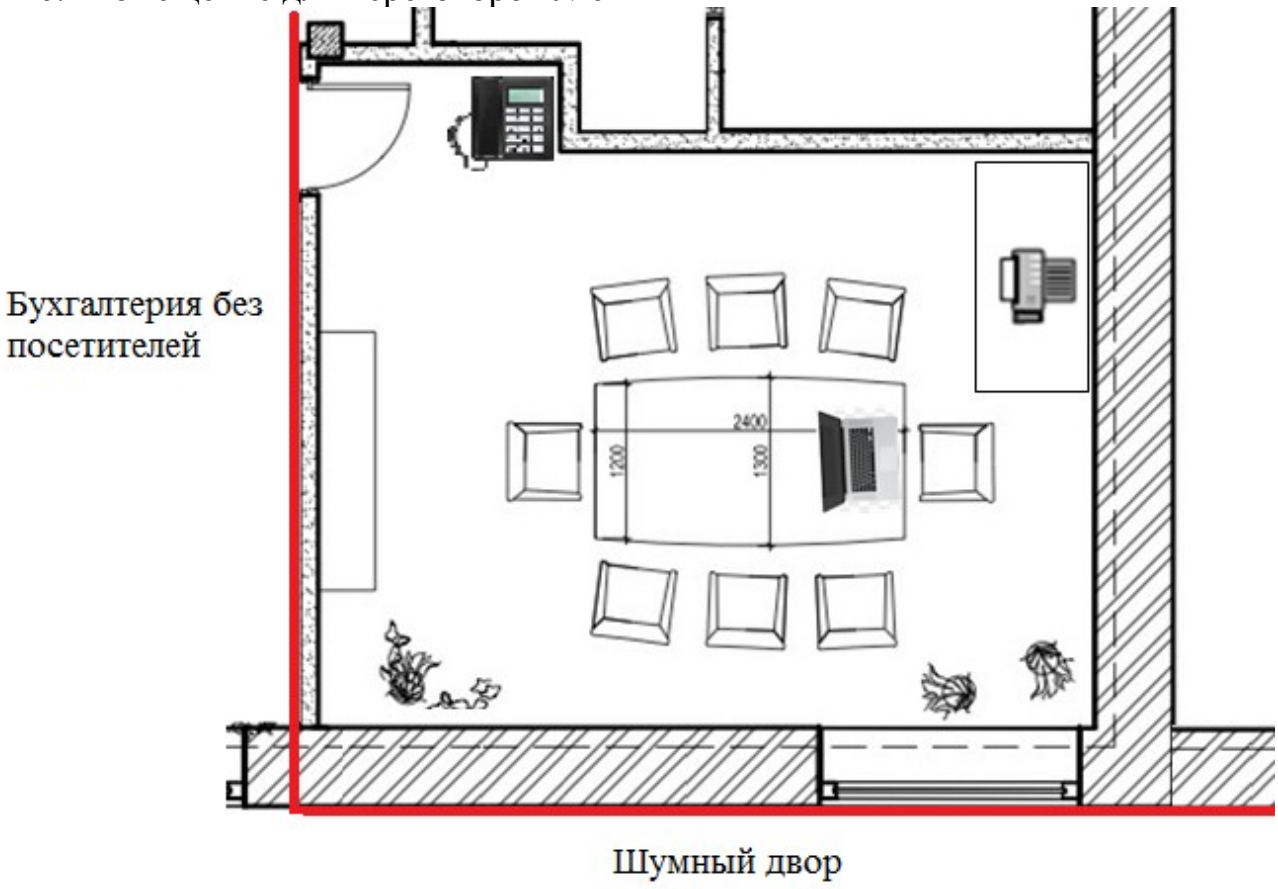
5. Помещение для переговоров №5



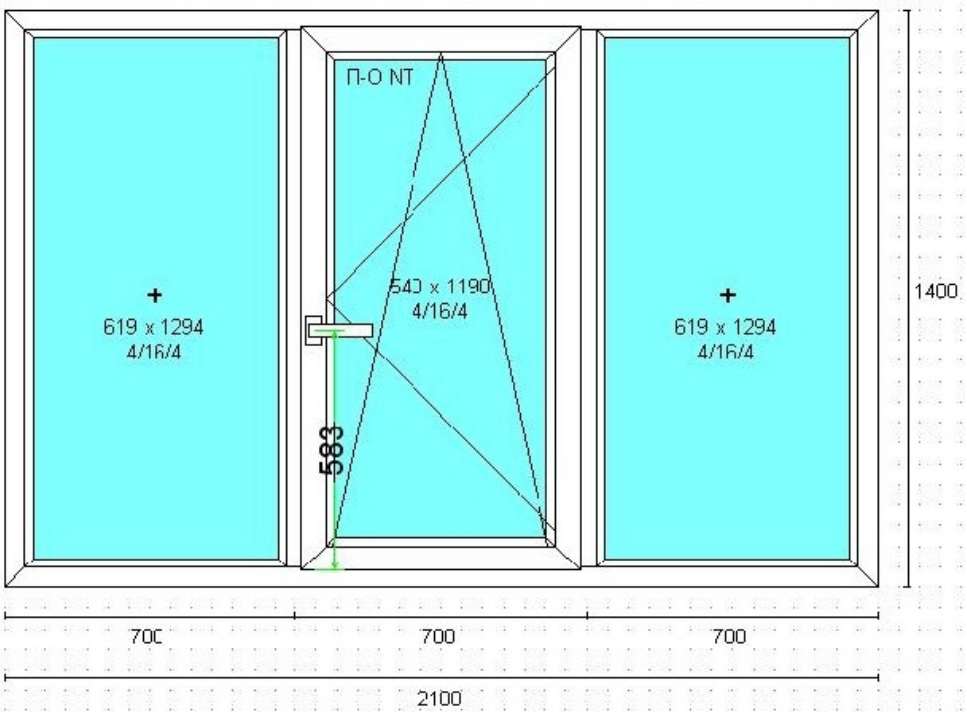
Ширина: 3820 мм, h=3000 мм
Размер окна:



6. Помещение для переговоров №6



Размеры: 4,5х6м, h=3,5м
Размер двери: 2х0,9м.



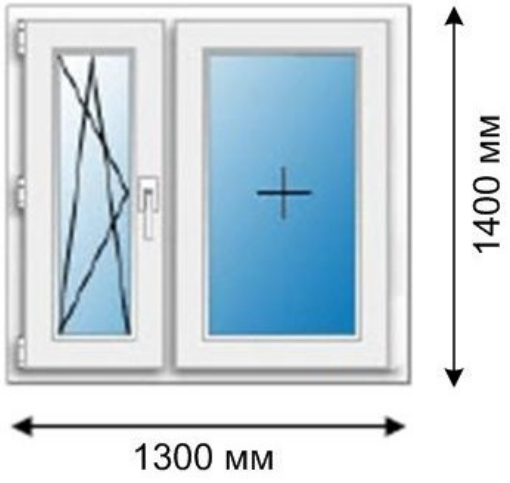
7. Помещение для переговоров №7

h=3,5m
Размер двери: 2х0,9м.

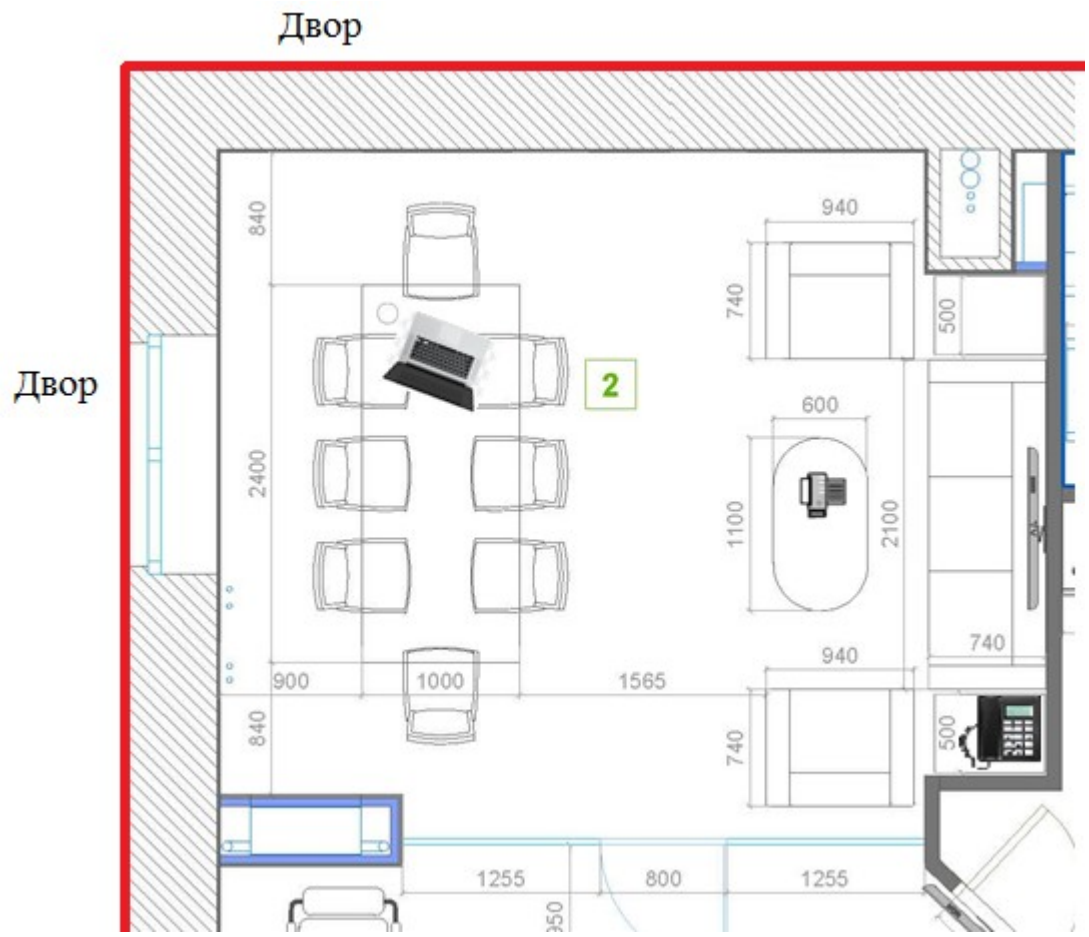
8. Помещение для переговоров №8

h=3м

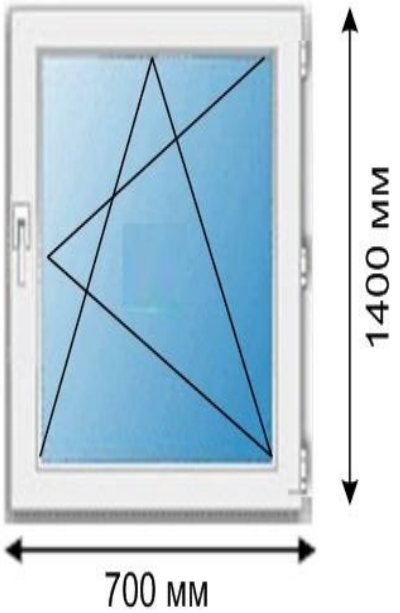
Размер двери: 2х0,9м.



9. Помещение для переговоров №9

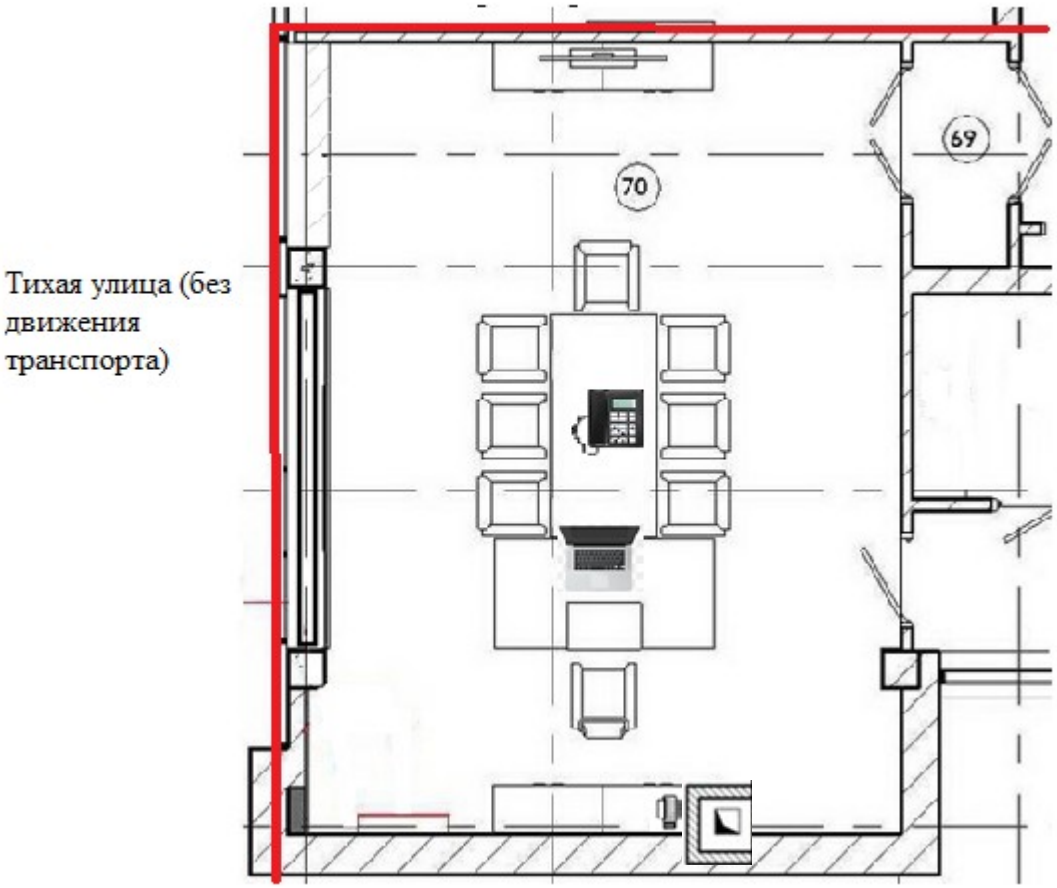


Размеры: 4,5х4,5м, h=3м.
Размер окна:



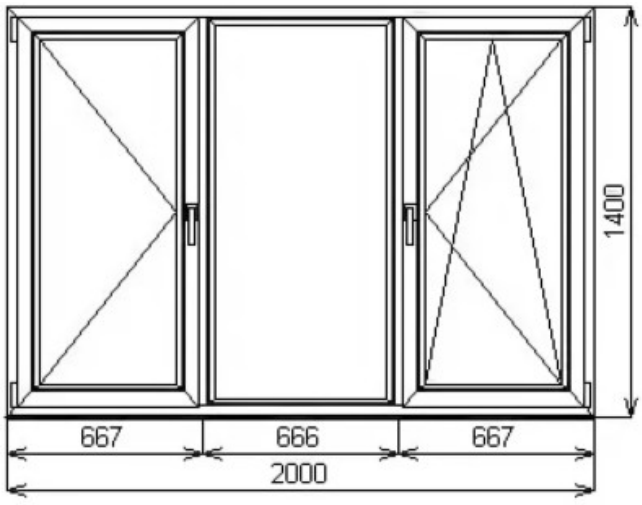
10.Помещение для переговоров №10

Кабинет при одном работающем



Размеры: 4,5х6,5м, h=3,5м.

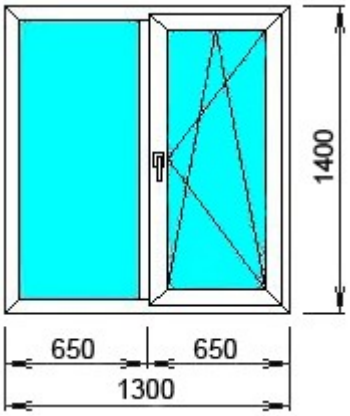
Размер окна:



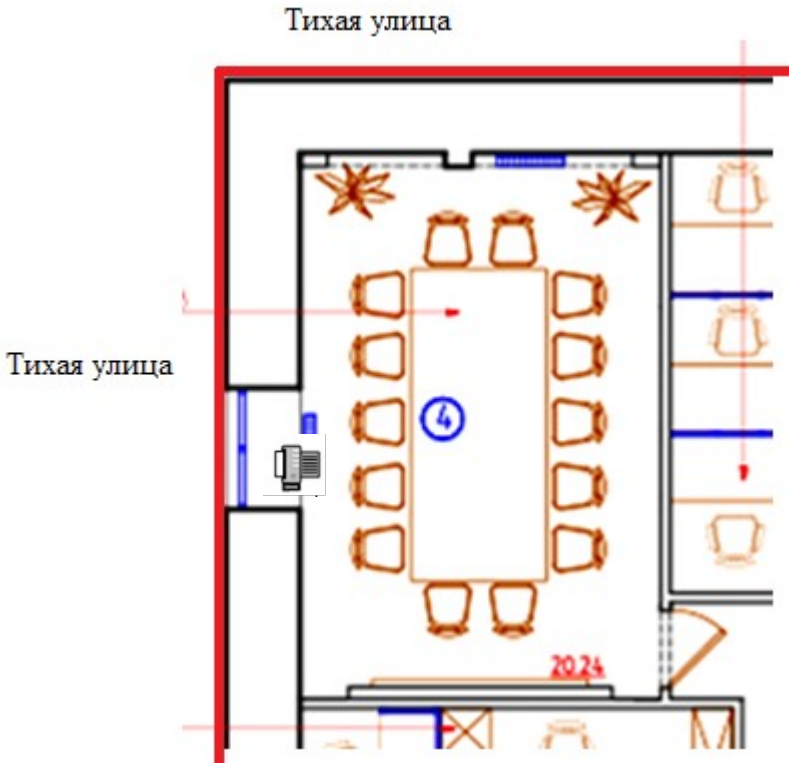
11.Помещение для переговоров №11

Размеры: 4,5х6,5м, h=3,5м.

Размер окна:

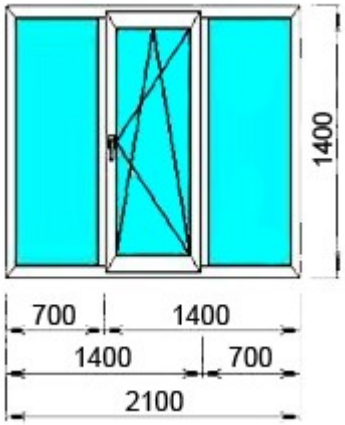


12.Помещение для переговоров №12



Размеры: 4,5х6,5м, h=3,5м.

Размер окна:



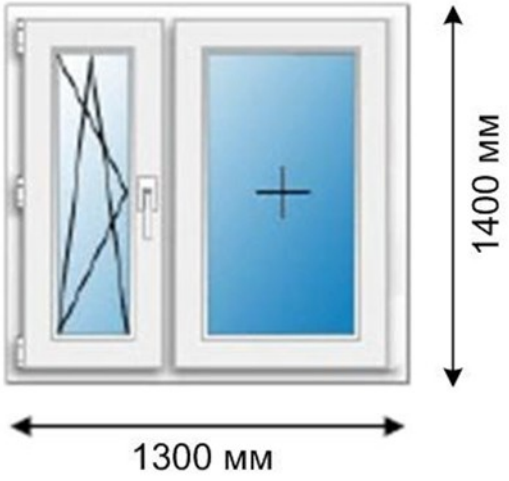
13.Помещение для переговоров №13

Размеры: 4,5х6,5м, h=3м.
Размер двери: 2х0,9м.

14.Помещение для переговоров №14

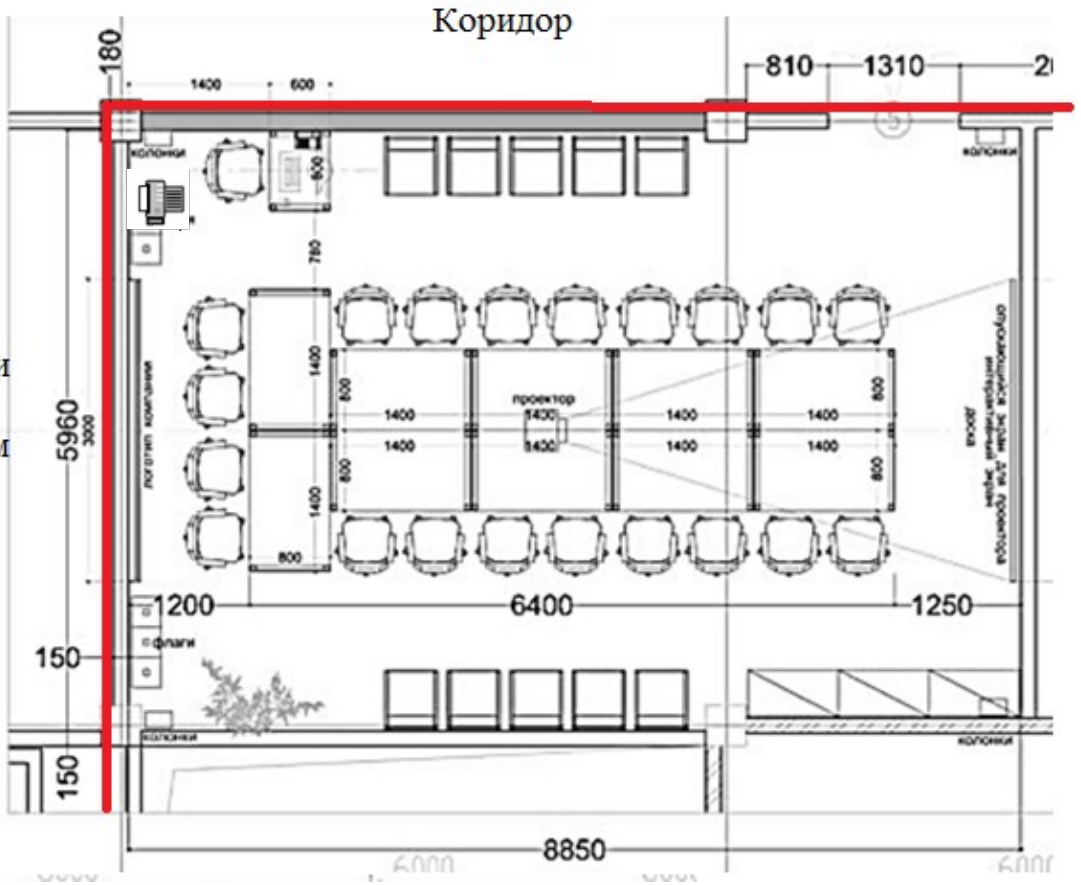
Размеры: 4,5х6,5м, h=3,5м.
Размер двери: 2х0,9м.

h=3,5m



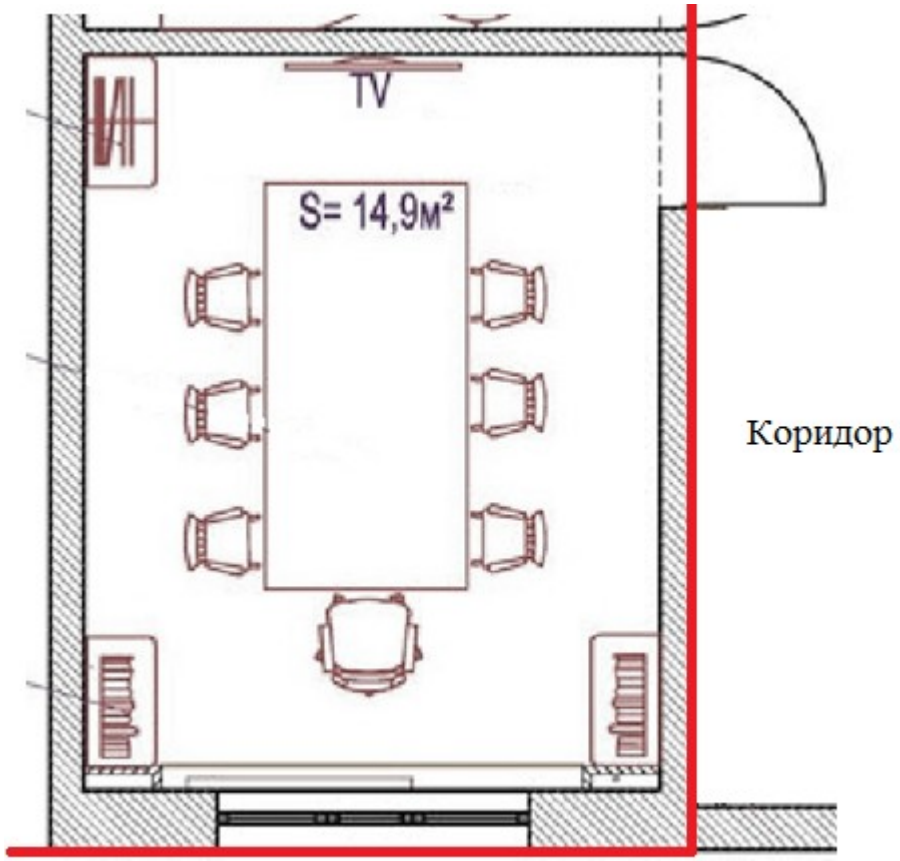
15.Помещение для переговоров №15

Кабинет при одном работающем

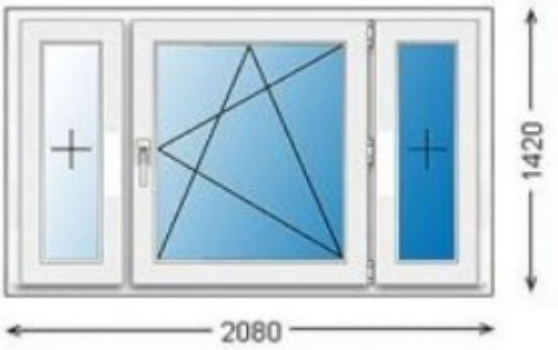


h=3,5м.
Размер двери: 2х0,9м.

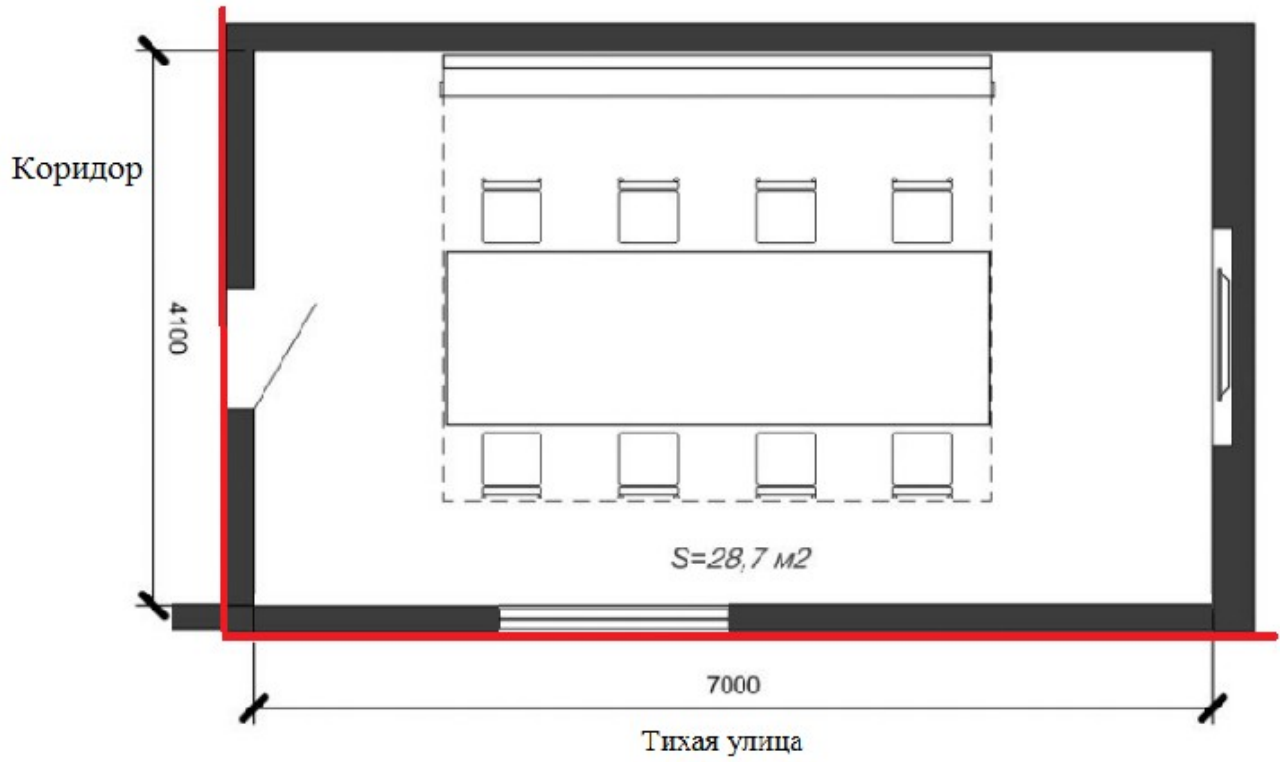
16.Помещение для переговоров №16



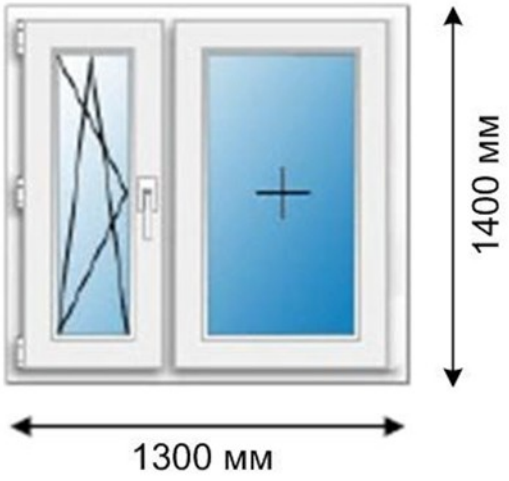
Размеры: 3х5м, h=3мм.
Размер двери: 2х0,9м.



17. Помещение для переговоров №17

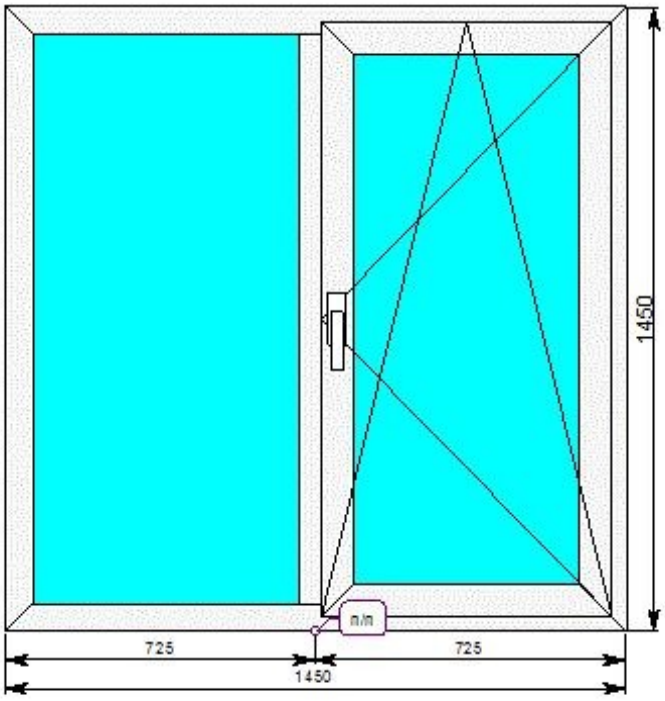


h=3,5м
Размер двери: 2х0,9м.

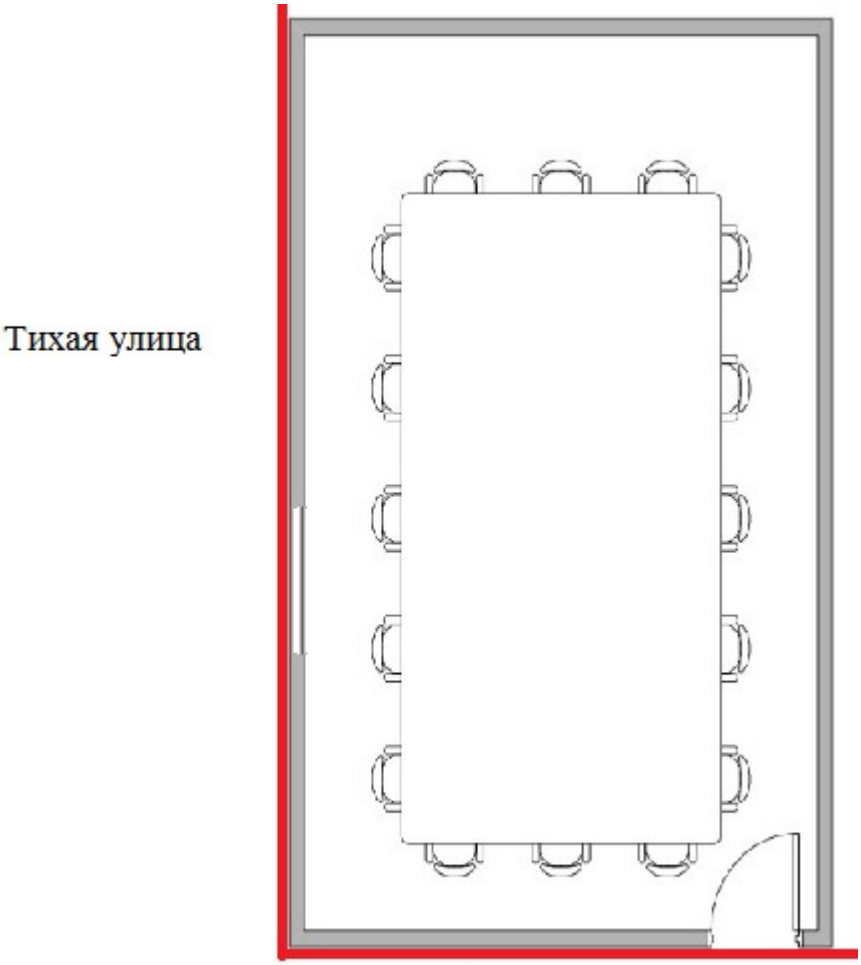


18.Помещение для переговоров №18

Размеры: 3х10м, h=3м.
Размер окна:

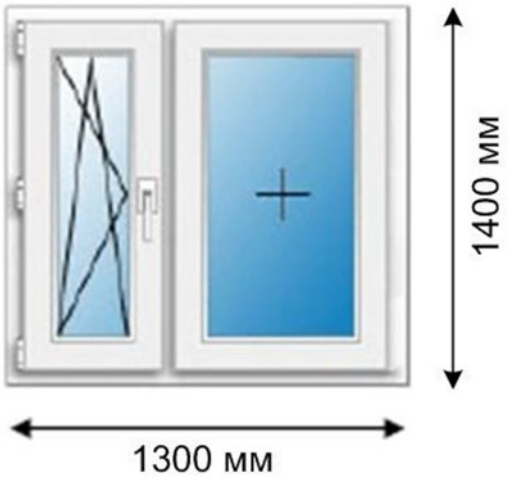


19.Помещение для переговоров №19

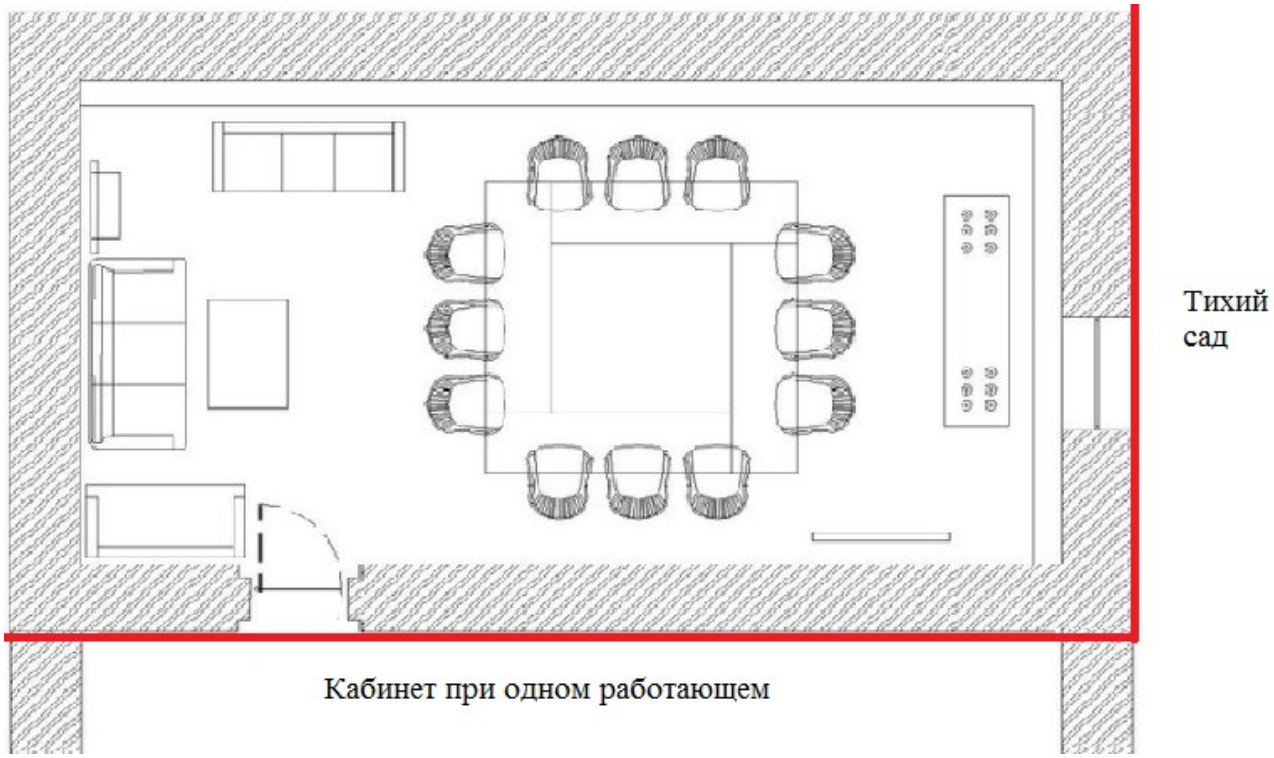


Комната тихая

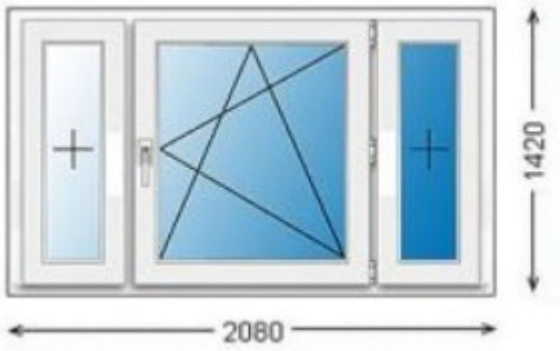
Размеры помещения: а=8м, в=4м, h=3,5м
Размер двери: 2х0,9м.



20.Помещение для переговоров №20



Размеры: 4х7м, h=3м
Размер двери: 2х0,9м.



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

для обучающихся по организации и проведению самостоятельной работы
по дисциплине «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»
для студентов направления подготовки **10.03.01 Информационная безопасность**
направленность (профиль) **Безопасность компьютерных систем**

Пятигорск, 2024

СОДЕРЖАНИЕ

1. Общие положения

Самостоятельная работа - планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

− формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

− написание докладов;

− подготовка к семинарам, практическим и лабораторным работам, их оформление;

− составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);

− выполнение учебно-исследовательских работ, проектная деятельность;

− подготовка практических разработок и рекомендаций по решению проблемной ситуации;

− выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;

− компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;

− выполнение курсовых работ (проектов) в рамках дисциплин;

− выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

● подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);

● основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);

● заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

Самостоятельная работа по дисциплине «Основы информационной безопасности» направлена на формирование следующих **компетенций**:

Код	Формулировка:
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности
ОПК-7	Способен использовать языки программирования и технологии разработки программах средств для решения задач профессиональной деятельности

2. Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование набора общенаучных, профессиональных и специальных компетенций будущего бакалавра по соответствующему направлению подготовки

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

● систематизация и закрепление полученных теоретических знаний и практических умений студентов;

● углубление и расширение теоретических знаний;

● формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;

● развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

● формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

● развитие исследовательских умений;

● использование материала, собранного и полученного в ходе самостоятельных занятий на семинарах, на практических и лабораторных занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к итоговым зачетам и экзаменам.

3. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе (акад.)		
			СРС	Контактная работа с преподавателем	Всего
ОПК-5 (ИД-1. ИД-2. ИД-3) ОПК-7(ИД-1. ИД-2. ИД-3)	Самостоятельное изучение литературы и источников	Собеседование	7,2	0,8	8
ОПК-5 (ИД-1. ИД-2. ИД-3) ОПК-7(ИД-1. ИД-2. ИД-3)	Подготовка к лабораторным работам	Защита ЛР	9,72	1,08	10,8
ОПК-5 (ИД-1. ИД-2. ИД-3) ОПК-7(ИД-1. ИД-2. ИД-3)	Подготовка к практическим занятиям	Защита ПР	6,48	0,72	7,2
ОПК-5 (ИД-1. ИД-2. ИД-3) ОПК-7(ИД-1. ИД-2. ИД-3)	Написание реферата/доклада	Защита доклада	9	1	10
		Итого	32,4	3,6	36

4. Порядок выполнения самостоятельной работы студентом

4.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют ***четыре основные установки в чтении научного текста***:

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;
2. Выделите главное, составьте план;

3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;

4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

4.2. Методические рекомендации по подготовке к практическим и лабораторным занятиям

Для того чтобы практические и лабораторные занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на практических занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

4.3. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала - умение решать задачи или пройти тестирование по пройденному материалу. Однако следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

4.4. Методические рекомендации по написанию научных текстов (докладов, докладовов, эссе, научных статей и т.д.)

Перед тем, как приступить к написанию научного текста, важно разобраться, какова истинная цель вашего научного текста - это поможет вам разумно распределить свои силы и время.

Во-первых, сначала нужно определиться с идеей научного текста, а для этого необходимо научиться либо относиться к разным явлениям и фактам несколько критически (своя идея – как иная точка зрения), либо научиться увлекаться какими-то известными идеями, которые нуждаются в доработке (идея – как оптимистическая позиция и направленность на дальнейшее совершенствование уже известного). Во-вторых, научиться организовывать свое время, ведь, как известно, свободное (от всяких глупостей) время – важнейшее условие настоящего творчества, для него наконец-то появляется время. Иногда именно на организацию такого времени уходит немалая часть сил и талантов.

Писать следует ясно и понятно, стараясь основные положения формулировать четко и недвусмысленно (чтобы и самому понятно было), а также стремясь структурировать свой текст. Каждый раз надо представлять, что ваш текст будет кто-то читать и ему захочется сориентироваться в нем, быстро находить ответы на интересующие вопросы (заодно представьте себя на месте такого человека). Понятно, что работа, написанная «сплошным текстом» (без заголовков, без выделения крупным шрифтом наиболее важным мест и т, п.), у культурного читателя должна вызывать брезгливость и даже жалость к автору (исключения составляют некоторые древние тексты, когда и жанр был иной и к текстам относились иначе, да и самих текстов было гораздо меньше – не то, что в эпоху «информационного взрыва» и соответствующего «информационного мусора»).

Объем текста и различные оформительские требования во многом зависят от принятых в конкретном учебном заведении порядков.

Доклад - это самостоятельное исследование студентом определенной проблемы, комплекса взаимосвязанных вопросов.

Доклад не должна составляться из фрагментов статей, монографий, пособий. Кроме простого изложения фактов и цитат, в доклад е должно проявляться авторское видение проблемы и ее решения.

Рассмотрим основные этапы подготовки

а студентом.

Выполнение доклада начинается с выбора темы.

Затем студент приходит на первую консультацию к руководителю, которая предусматривает:

- обсуждение цели и задач работы, основных моментов избранной темы;
- консультирование по вопросам подбора литературы;
- составление предварительного плана.

Следующим этапом является работа с литературой. Необходимая литература подбирается студентом самостоятельно.

После подбора литературы целесообразно сделать рабочий вариант плана работы. В нем нужно выделить основные вопросы темы и параграфы, раскрывающие их содержание.

Составленный список литературы и предварительный вариант плана уточняются, согласуются на очередной консультации с руководителем.

Затем начинается следующий этап работы - изучение литературы. Только внимательно читая и конспектируя литературу, можно разобраться в основных вопросах темы и подготовиться к самостоятельному (авторскому) изложению содержания доклада. Конспектируя первоисточники, необходимо отразить основную идею автора и его позицию по исследуемому вопросу, выявить проблемы и наметить задачи для дальнейшего изучения данных проблем.

Систематизация и анализ изученной литературы по проблеме исследования позволяют студенту написать работу.

Рабочий вариант текста доклада предоставляется руководителю на проверку. На основе рабочего варианта текста руководитель вместе со студентом обсуждает возможности доработки текста, его оформление. После доработки доклад сдается на кафедру для его оценивания руководителем.

Требования к написанию доклада

Написание 1 доклада является обязательным условием выполнения плана СРС по любой дисциплине профессионального цикла.

Тема доклада может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Доклад должен быть написан научным языком.

Объем доклада должен составлять 20-25 стр.

Структура доклада:

● Введение (не более 3-4 страниц). Во введении необходимо обосновать выбор темы, ее актуальность, очертить область исследования, объект исследования, основные цели и задачи исследования.

● Основная часть состоит из 2-3 разделов. В них раскрывается суть исследуемой проблемы, проводится обзор мировой литературы и источников Интернет по предмету исследования, в котором дается характеристика степени разработанности проблемы и авторская аналитическая оценка основных теоретических подходов к ее решению. Изложение материала не должно ограничиваться лишь описательным подходом к раскрытию выбранной темы. Оно также должно содержать собственное видение рассматриваемой проблемы и изложение собственной точки зрения на возможные пути ее решения.

● Заключение (1-2 страницы). В заключении кратко излагаются достигнутые при изучении проблемы цели, перспективы развития исследуемого вопроса

● Список использованной литературы (не меньше 10 источников), в алфавитном порядке, оформленный в соответствии с принятыми правилами. В список использованной литературы рекомендуется включать работы отечественных и зарубежных авторов, в том числе статьи, опубликованные в научных журналах в течение последних 3-х лет и ссылки на ресурсы сети Интернет.

● Приложение (при необходимости).

Требования к оформлению:

● текст с одной стороны листа;

● шрифт Times New Roman;

● кегль шрифта 14;

● межстрочное расстояние 1,5;

● поля: сверху 2,5 см, снизу – 2,5 см, слева - 3 см, справа 1,5 см;

● доклад должен быть представлен в сброшюрованном виде.

Порядок защиты доклада:

Защита доклада проводится на практических занятиях, после окончания работы студента над ним и исправления всех недочетов, выявленных преподавателем в ходе консультаций. На защиту доклада отводится 5-7 минут времени, в ходе которого студент должен показать свободное владение материалом по заявленной теме. При защите доклада приветствуется использование мультимедиа-презентации.

Оценка доклада

Доклад оценивается по следующим критериям:

• соблюдение требований к его оформлению;

• необходимость и достаточность для раскрытия темы приведенной в тексте доклада информации;

• умение студента свободно излагать основные идеи, отраженные в докладе;

• способность студента понять суть задаваемых преподавателем и сокурсниками вопросов и сформулировать точные ответы на них.

Критерии оценки:

Оценка «отлично» выставляется студенту, если в докладе студент исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует для написания доклада современные научные материалы; анализирует полученную информацию; проявляет самостоятельность при написании доклада.

Оценка «хорошо» выставляется студенту, если качество выполнения доклада достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопросы по теме доклада.

Оценка «удовлетворительно» выставляется студенту, если материал доклада излагается частично, но пробелы не носят существенного характера, студент допускает неточности и ошибки при защите доклада, дает недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении материала.

Оценка «неудовлетворительно» выставляется студенту, если он не подготовил доклад или допустил существенные ошибки. Студент неуверенно излагает материал доклада, не отвечает на вопросы преподавателя.

Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным 55. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.5. Методические рекомендации по выполнению исследовательских проектов

Исследовательская проектная работа – это групповая работа, для выполнения которой необходим выбор и приложение научной методики к поставленной задаче, получение собственного теоретического или экспериментального материала, на основании которого необходимо провести анализ и сделать выводы об исследуемом явлении. Выполнение проекта – это всегда коллективная, творческая практическая работа, предназначенная для получения определенного продукта или научно-технического результата. Такая работа подразумевает четкое, однозначное формирование поставленной задачи, определение сроков выполнения намеченного, определение требований к разрабатываемому объекту.

Выполнение 1 группового проекта является обязательным условием выполнения самостоятельной работы по любой дисциплине профессионального цикла. Тема проектного задания может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Требования по выполнению и оформлению проекта

При выполнении проекта приветствуется работа в группе (2-3 человека). Проект – это исследовательская работа, в ходе которой студенты должны продемонстрировать владение навыками научного исследования, умения проводить анализ, обобщать информацию, делать выводы, предлагать свои решения проблемы, рассматриваемой в проекте.

При подготовке материалов проекта студенты должны продемонстрировать владение современными методами компьютерной обработки данных.

Критерии оценки работы участника проекта.

Для каждого из участников проекта оцениваются:

• профессиональные теоретические знания в соответствующей области;

• умение работать со справочной и научной литературой, осуществлять поиск необходимой информации в Интернет;

• умение работать с техническими средствами;

• умение пользоваться соответствующими выполняемому проекту информационными технологиями;

• умение готовить материалы проекта для презентации: составлять и редактировать тексты, формировать презентацию проекта;

• умение работать в команде;

• умение публично представлять результаты собственной деятельности;

• коммуникабельность, инициативность, творческие способности.

Критерии выставления оценки участникам проекта

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
«Отлично»	Работа выполнена на	Технические	Студент проявил	Проект

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
	высоком профессиональном уровне. Представленный материал в основном фактически верен, допускаются негрубые фактические неточности. Студент свободно отвечает на вопросы, связанные с проектом.	средства и информационные технологии освоены и использованы для реализации проекта полностью	инициативу, творческий подход, способность к выполнению сложных заданий, навыки работы в коллективе, организационные способности.	представлен полностью и в срок.
«Хорошо»	Работа выполнена на достаточно высоком профессиональном уровне. Допущено до 4–5 фактических ошибок. Студент отвечает на вопросы, связанные с проектом, но недостаточно полно.	Обнаруживаются некоторые ошибки в использовании соответствующих технических средств и информационных технологий	Студент достаточно полно, но без инициативы и творческих находок выполнил возложенные на него задачи.	Проект представлен достаточно полно и в срок, но с некоторыми недоработками.
«Удовлетворительно»	Уровень недостаточно высок. Допущено до 8 фактических ошибок. Студент может ответить лишь на некоторые из заданных вопросов, связанных с проектом.	Обнаруживает недостаточное владение навыками работы с техническими средствами и соответствующими информационными технологиями	Студент выполнил большую часть возложенной на него работы.	Проект сдан со значительным опозданием (более недели) и не полностью
«Неудовлетворительно»	Работа не выполнена или выполнена на низком уровне. Допущено более 8 фактических ошибок. Ответы на	Навыков работы с техническими средствами нет, информационные технологии не освоены	Студент практически не работал, не выполнил свои задачи или выполнил лишь	Проект не сдан.

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
	связанные с проектом вопросы обнаруживают непонимание предмета и отсутствие ориентации в материале проекта.		отдельные не существенные поручения в групповом проекте.	

Студенты должны: защитить проект в режиме презентации, предъявить файлы выполненного проекта, уметь рассказать о технологиях, использованных ими при выполнении проекта, дать оценку работы каждого члена группы (*если проект групповой*).

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.6. Методические рекомендации по подготовке к экзаменам и зачетам

Изучение многих общепрофессиональных и специальных дисциплин завершается экзаменом. Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине.

Экзаменационная сессия - это серия экзаменов, установленных учебным планом. Между экзаменами интервал 3-4 дня. Не следует думать, что 3-4 дня достаточно для успешной подготовки к экзаменам.

В эти 3-4 дня нужно систематизировать уже имеющиеся знания. На консультации перед экзаменом студентов познакомят с основными требованиями, ответят на возникшие у них вопросы. Поэтому посещение консультаций обязательно.

Требования к организации подготовки к экзаменам те же, что и при занятиях в течение семестра, но соблюдаться они должны более строго. Во-первых, очень важно соблюдение режима дня; сон не менее 8 часов в сутки, занятия заканчиваются не позднее, чем за 2-3 часа до сна. Оптимальное время занятий - утренние и дневные часы. В перерывах между занятиями рекомендуются прогулки на свежем воздухе, неутомительные занятия спортом. Во-вторых, наличие хороших собственных конспектов лекций. Даже в том случае, если была пропущена какая-либо лекция, необходимо во время ее восстановить (переписать ее на кафедре), обдумать, снять возникшие вопросы для того, чтобы запоминание материала было осознанным. В-третьих, при подготовке к экзаменам у студента должен быть хороший учебник или конспект литературы, прочитанной по указанию преподавателя в течение семестра. Здесь можно эффективно использовать листы опорных сигналов.

Вначале следует просмотреть весь материал по сдаваемой дисциплине, отметить для себя трудные вопросы. Обязательно в них разобраться. В заключение еще раз целесообразно повторить основные положения, используя при этом листы опорных сигналов.

Систематическая подготовка к занятиям в течение семестра позволит использовать время экзаменационной сессии для систематизации знаний.

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, оценка доклада, оценка презентации, оценка участия в круглом столе, оценка выполнения проекта.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

Список литературы для выполнения СРС

Основная литература:

1. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 c. - Книга находится в базовой версии ЭБС IPRbooks., экземпляров неограниченно

2. Нестеров С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Нестеров С.А.— Электрон. текстовые данные.— СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014.— 322 c.- Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-87623-969-3, экземпляров неограниченно

Дополнительная литература:

1. Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Элек-тронный ресурс]/ Фаронов А.Е.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 154 c. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 978-5-9500999-7-7, экземпляров неограниченно

2. Защита информации в операционных системах: учеб.пособие.- Ставрополь: Изд-во СГУ, 2015.- 318 с - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-91359-219-4, экземпляров неограниченно

Методическая литература:

1. Методические рекомендации по выполнению практических работ по дисциплине "Основы информационной безопасности"

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине "Основы информационной безопасности"

Интернет-ресурсы:

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Цифровая грамотность и обработка больших данных»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.