

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шебзухова Татьяна Александровна
Должность: Директор Пятигорского института (филиал) Северо-Кавказского
федерального университета
Дата подписания: 05.10.2023 15:21:44
Уникальный программный ключ:
d74ce93cd40e39275c3ba2f58486412a1c8ef96f

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

«Информационная безопасность в системе экономической безопасности»

для студентов специальности **38.05.01 Экономическая безопасность**

специализация **Защита национальных интересов Российской Федерации в
экономической и внешнеэкономической сфере**

Пятигорск
2023

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ.....	2
2. ОБОРУДОВАНИЕ И МАТЕРИАЛЫ	2
3. УКАЗАНИЯ ПО ТЕХНИКЕ БЕЗОПАСНОСТИ	2
4. СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ РАБОТ	3
Практическая работа №1. Оценка рисков информационной безопасности на основе методики OSTATE	3
Практическая работа №2. Разработка политики информационной безопасности предприятия: верхний уровень.....	11
Практическая работа №3. Разработка политики информационной безопасности предприятия: средний уровень	14
Практическая работа №4. Определение класса автоматизированной системы	17
Практическая работа №5. Определение требований по защите информации от НСД для АС	20
Практическая работа №6. Правила формирования паролей	21
Практическая работа №7. Защита баз данных на примере MS ACCESS с помощью пароля	24
Практическая работа №8. Утечка речевой информации. Определение звукоизоляции ограждающих конструкций	29
Практическая работа №9. Утечка речевой информации. Определение уровня шумов и акустических сигналов	36
ПРИЛОЖЕНИЕ А	41
ПРИЛОЖЕНИЕ Б	42
ПРИЛОЖЕНИЕ В.....	44
ПРИЛОЖЕНИЕ Г	47
ПРИЛОЖЕНИЕ Е	76
ПРИЛОЖЕНИЕ Ж.....	77

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 «Информационная безопасность в системе экономической 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 общепрофессиональных компетенций будущего специалиста по специальности 38.05.01 Экономическая 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 практических 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, окрашивать 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,

ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 2C0000041E9AB8B932205E7B7A30000000043E
Владелец: Владимир Владимирович Алехин
Действителен: с 19.08.2022 по 19.08.2023

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

Практическая работа №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.

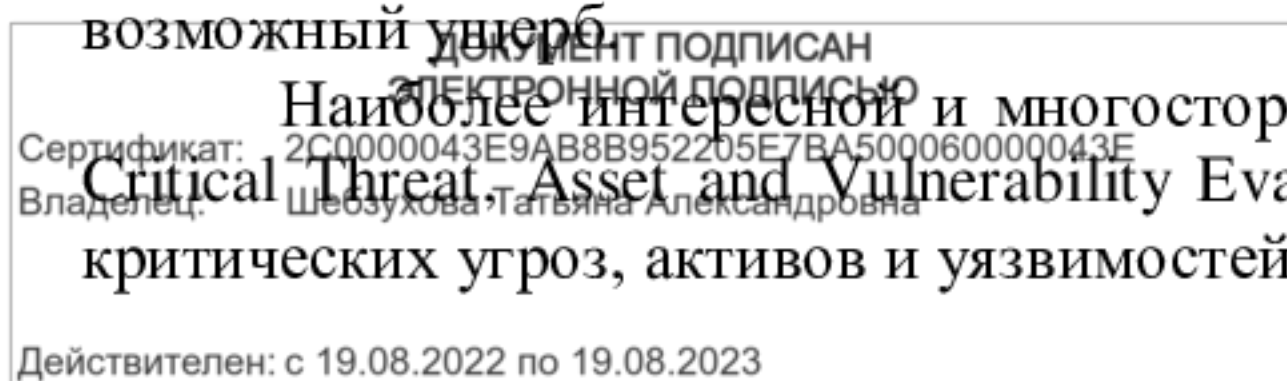
На практике наибольшее распространение получили два подхода к обоснованию проекта подсистемы обеспечения безопасности.

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 OSTAVE 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 OSTAVE

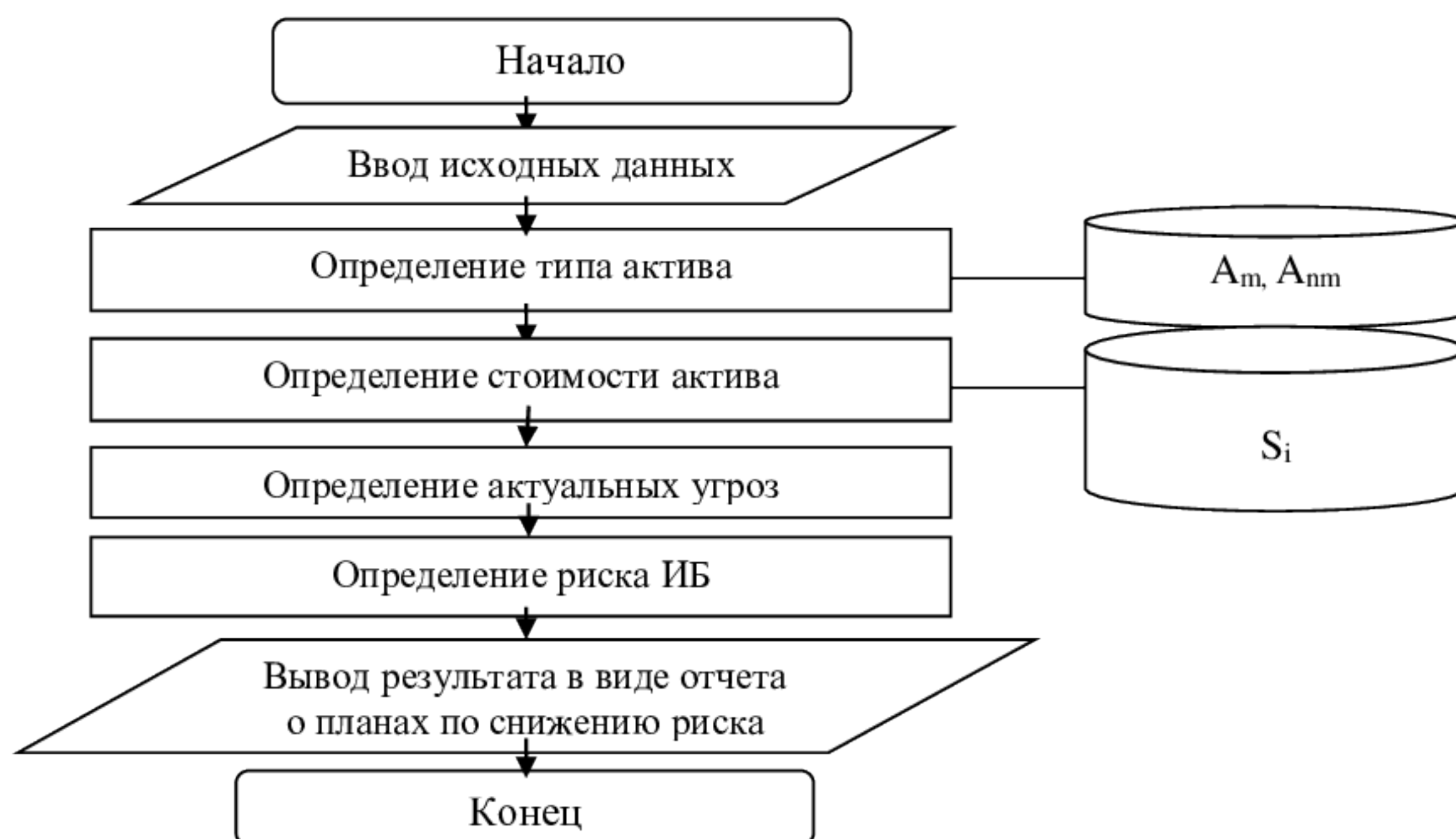


Рис. 1.

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

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).

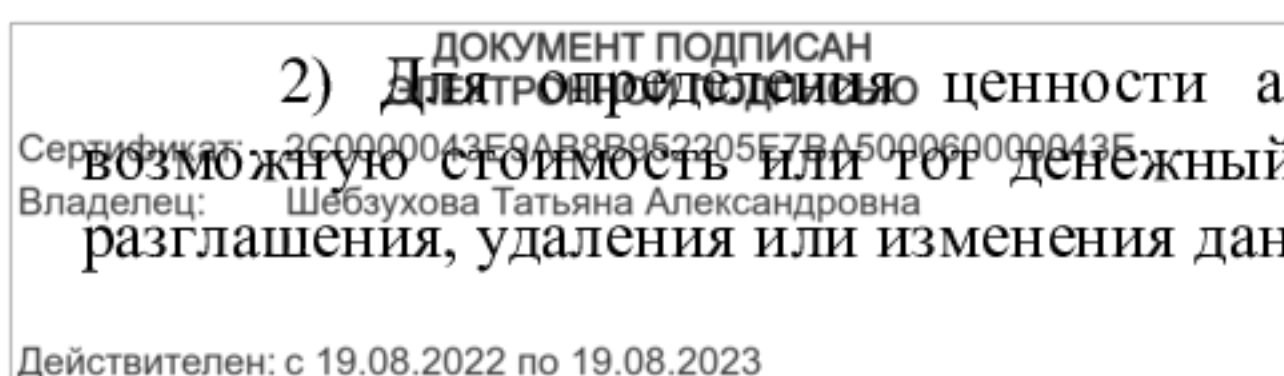
Таблица 1.

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	Комплекующие 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

Сертификат:
Владелец: 2C0000043E9AB8B952205E7BA500060000043E
Шебухова Татьяна Александровна

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Действителен: с 19.08.2022 по 19.08.2023

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 - $V_{г\text{у}}$. 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	+	

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебухова Татьяна Александровна

19 – 100%
Действителен: с 19.08.2022 по 19.08.2023

10 – x%

1000/19=53%

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

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

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

- $V_{гy}=10$ - 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, $V_{гy}=5$.

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

$$R = S * V_{гy}, \quad (1)$$

где:

$V_{гy}$ – вероятность реализации угрозы;

S – ценность всех активов, определяемое выражением:

$$S = \sum_{i=0}^n S_i, \quad (2)$$

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 ($V_{гy}$).

Таблица 5. Определение величины риска ИБ

	R						
$V_{гy}$	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 $V_{гy} = 5$ 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 ($V_{гy}$). План по снижению риска: на среднюю перспективу

Таблица 6. Определение временных значений риска ИБ

$V_{гy}$	План по снижению риска
1	Долговременный
5	На среднюю перспективу

Сертификат: 2C0000043E9AB8B952205E7BBA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

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 OBTAVE 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 _{гy} = 5	R=40	Средняя	На среднюю перспективу

В отличие от прочих методик, OBTAVE не предполагает привлечения для исследования безопасности ИС сторонних экспертов, а вся документация по OBTAVE 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 OBTAVE 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_{гy} (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				+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
4	Система видеонаблюдения						+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
	Система охранной сигнализации						+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
4	Экранирование							+	+	+	+	+	+	+	+	+	+	+	+	+	+

Сертификат:
Владелец:

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
2C0000043E9AB8B932205E7BA500060000043E

Действителен: с 19.08.2022 по 19.08.2023

№ п/п	Средство нейтрализации угрозы	Варианты с имеющимися на объекте средствами защиты																	
	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, 2012. – №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.

Электронная подпись
Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шинаков К.Е.
Действителен: с 19.08.2022 по 19.08.2023

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: <http://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.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

- 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.

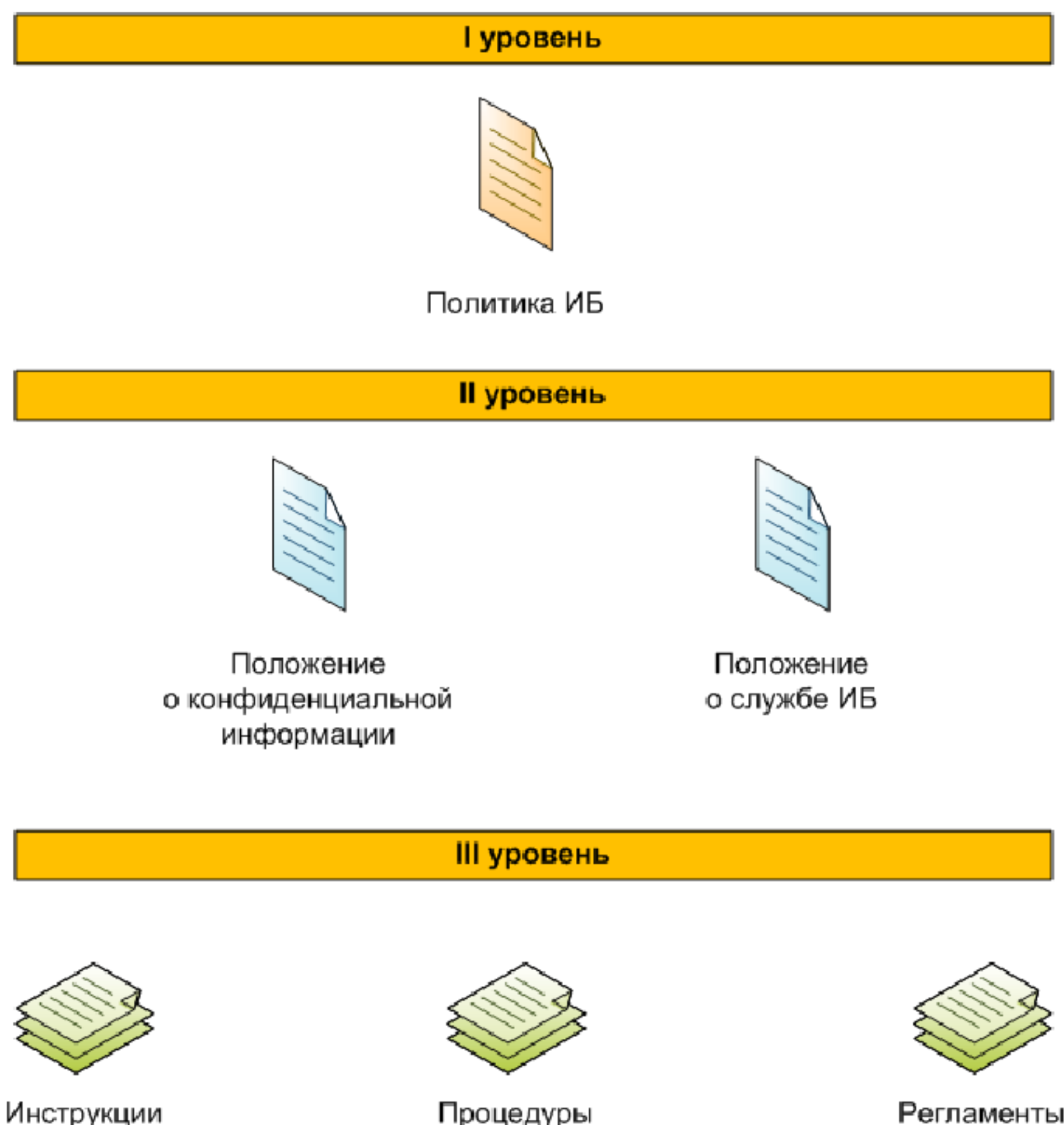


Рисунок 1. Структура нормативно-методических документов в области ИБ

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 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 ИБ 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.

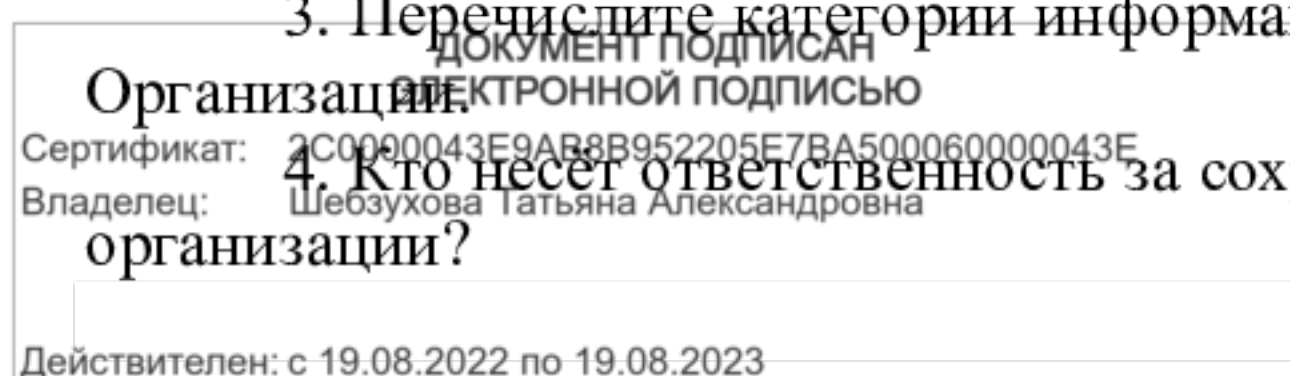
- 2) Оформить отчёт.
- 3) Ответить на контрольные вопросы.
- 4) Сделать вывод.

Контрольные вопросы:

1. Кто утверждает все оформленные решения, формирующие ИБ?
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: <http://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.

Практическая работа №3. Разработка политики информационной безопасности предприятия: средний уровень

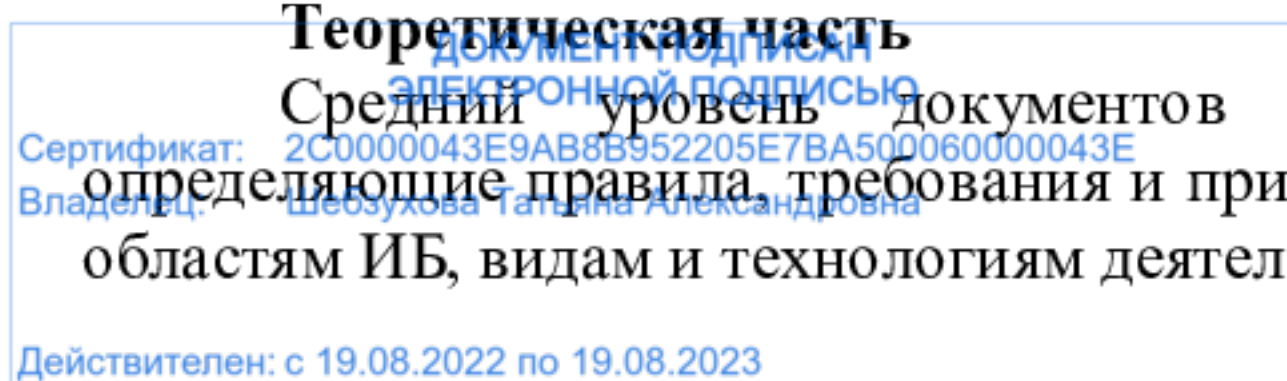
Цель работы: изучить существующие стандарты международного и отечественного уровня в области построения политики безопасности.

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 отчет.
- 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

Сертификат:
Владелец:

ЭЛЕКТРОННОЙ ПОДПИСЬЮ
2C0000043E9AB8B952205E7BA500060000043E
Шифр ключа Александра Александровна

Действителен: с 19.08.2022 по 19.08.2023

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](http://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.

Практическая работа №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.

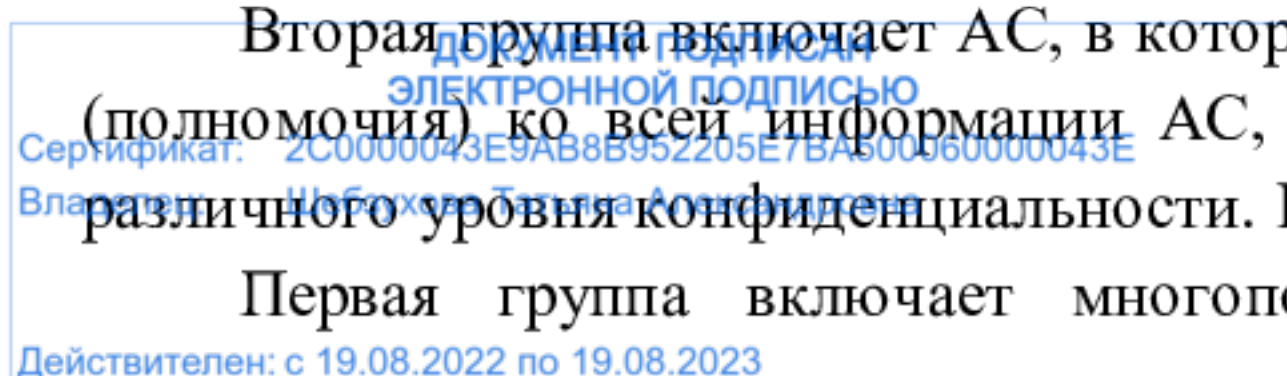
Устанавливается девять классов защищенности АС от НСД к информации.

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

Сертификат: 2C0000043B7A88B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

		информации АС	
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 отчета и его форма

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E

Владелец: Шебзухова Татьяна Александровна

Отчет по лабораторной работе оформляется в программной оболочке Microsoft Word

Действителен: с 19.08.2022 по 19.08.2023

(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.

Защита 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?

Практическая работа №5. Определение требований по защите информации от НСД для АС

Цель работы: научиться 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.

Защита 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?

Практическая работа №6. Правила формирования паролей

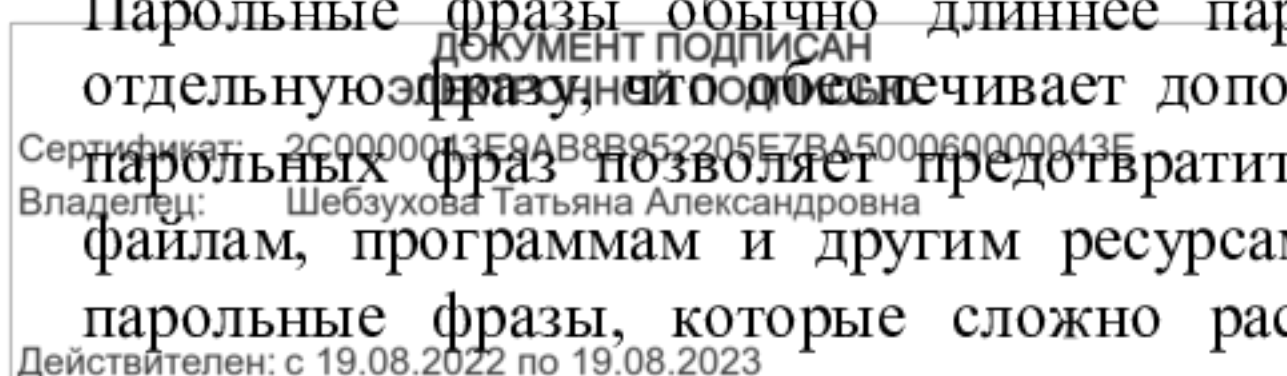
Цель работы: научиться формировать пароли пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.

1. Теоретическая часть

Для выполнения мероприятия идентификация и аутентификация субъектов доступа и объектов доступа потребуются 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



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.

Признаки надежных паролей и парольных фраз

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

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	` ~ ! @ # \$ % ^ & * () _ - + = { } [] \ : ; " ' < > , . ? /

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».

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 надёжную парольную фразу м0й \$ыН р0дНлс' 12124. Пароли и парольные фразы могут быть связаны с любимым видом спорта или хобби. Например, Мне нравится играть в бадминтон можно переделать в Мн€НрА8№тсЯ№грАт'вБадДм№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.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 290000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

3. Задание.

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

Действителен: с 19.08.2022 по 19.08.2023

- #### 4. Содержание отчета и его форма:

Отчет по лабораторной работе должен состоять из следующих структурных элементов:

- Защита 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

- ## Практическая работа №7. Защита баз данных на примере MS ACCESS с помощью пароля

1. Основы теории

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

критериям, полученные отчетов. Данные
элементов, которые называются элементами,
предназначены для отображения полей
объекта. Чтобы автоматизировать досту
Действителен: с 19.08.2022 по 19.08.2023

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.

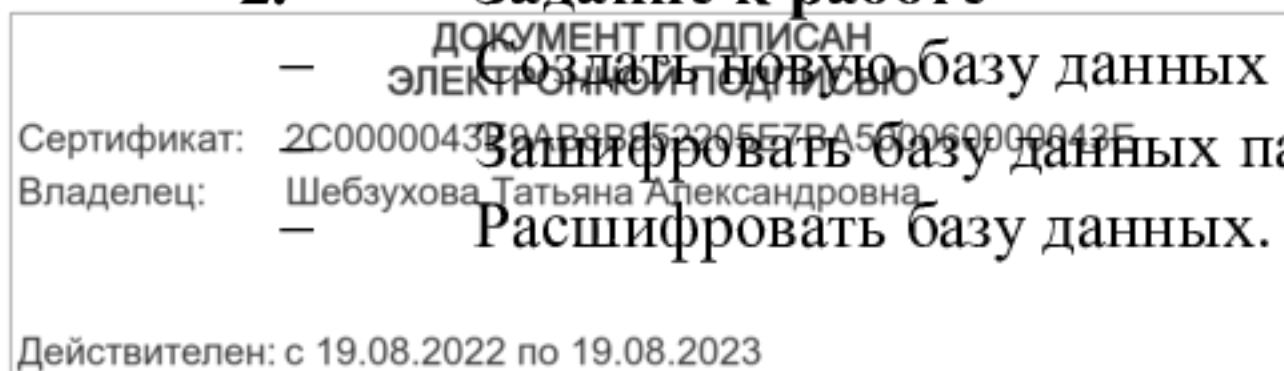
В более ранних версиях Access вы можете создать учетные записи пользователей и пароли с помощью функции безопасности на уровне пользователя. Зашифрованную базу данных, пароль от которой утерян, невозможно использовать. Если пароль неизвестен, его нельзя удалить. Функция шифрования действует только в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

2. Задание к работе

— Создать новую базу данных MS Access.

— Зашифровать базу данных паролем.

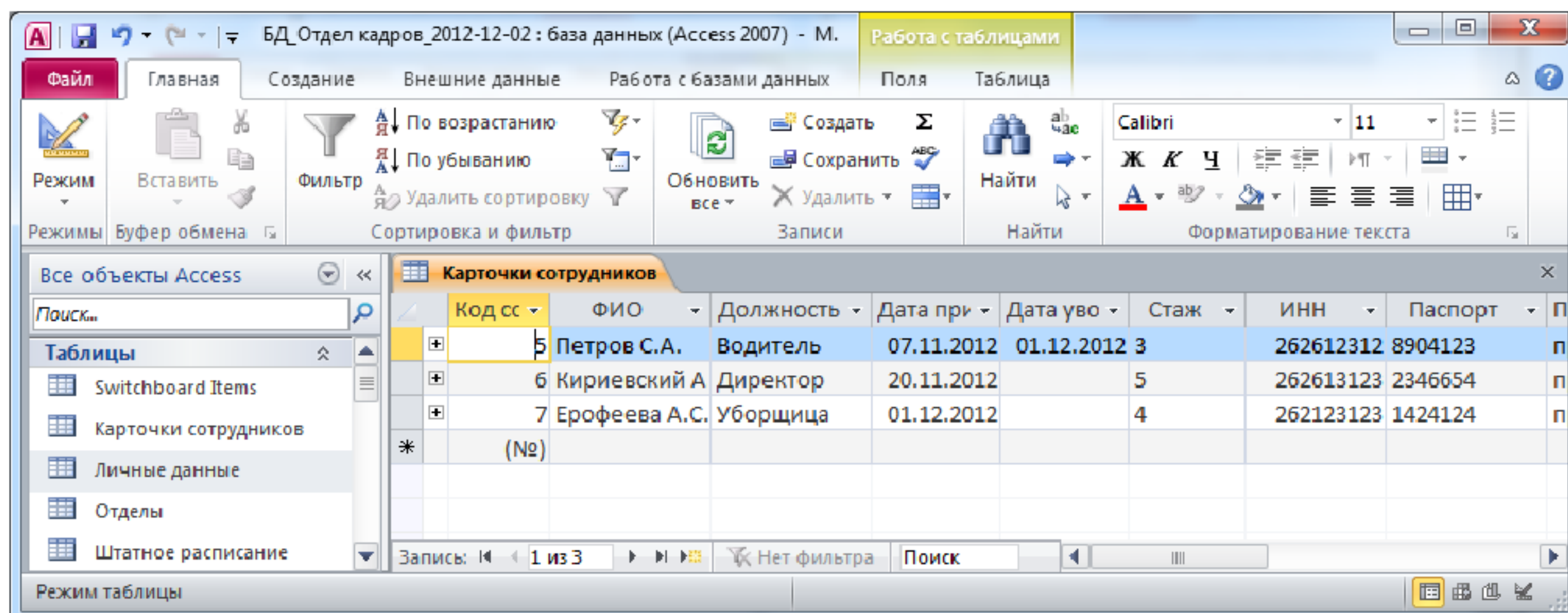
— Расшифровать базу данных.



3. Порядок выполнения работы

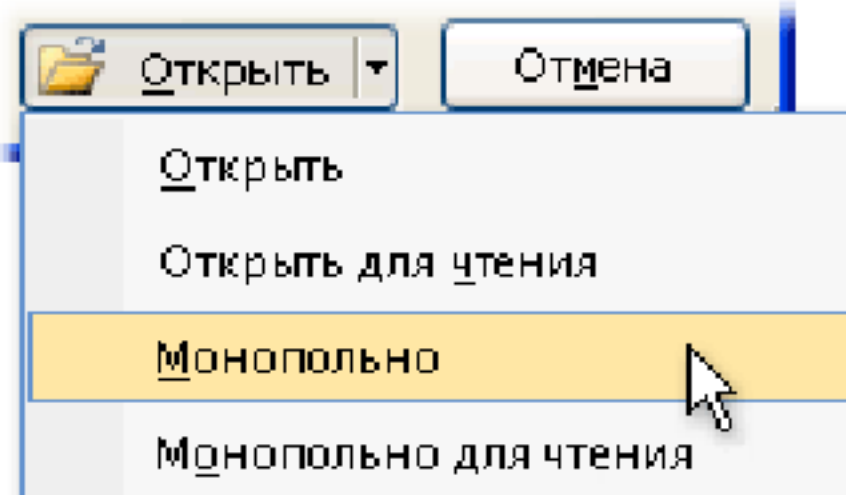
В Access 2010 не поддерживается защита на уровне пользователя для баз данных, созданных в новом формате (ACCDB и ACCDE-файлы). Однако при открытии базы данных из более ранней версии Access, имеющей защиту на уровне пользователя, в Access 2010 эти параметры будут продолжать действовать. Поэтому рассмотрим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

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

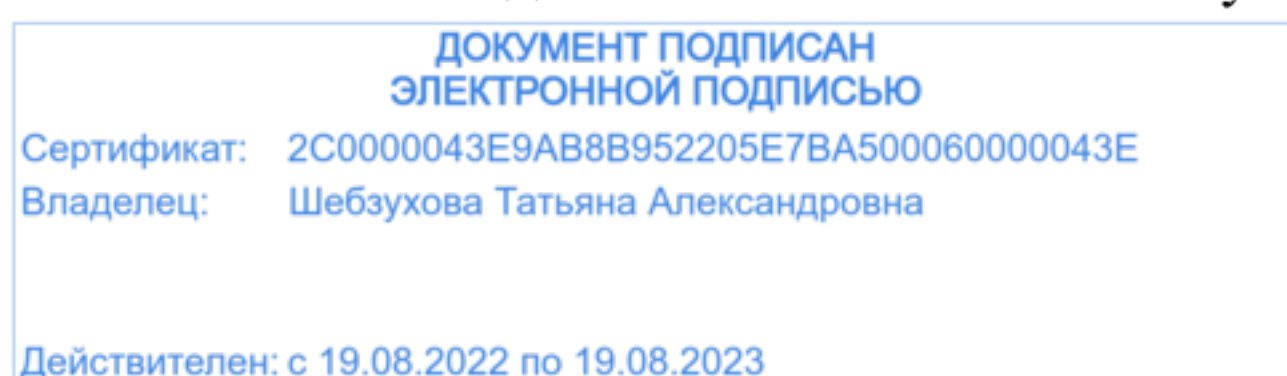


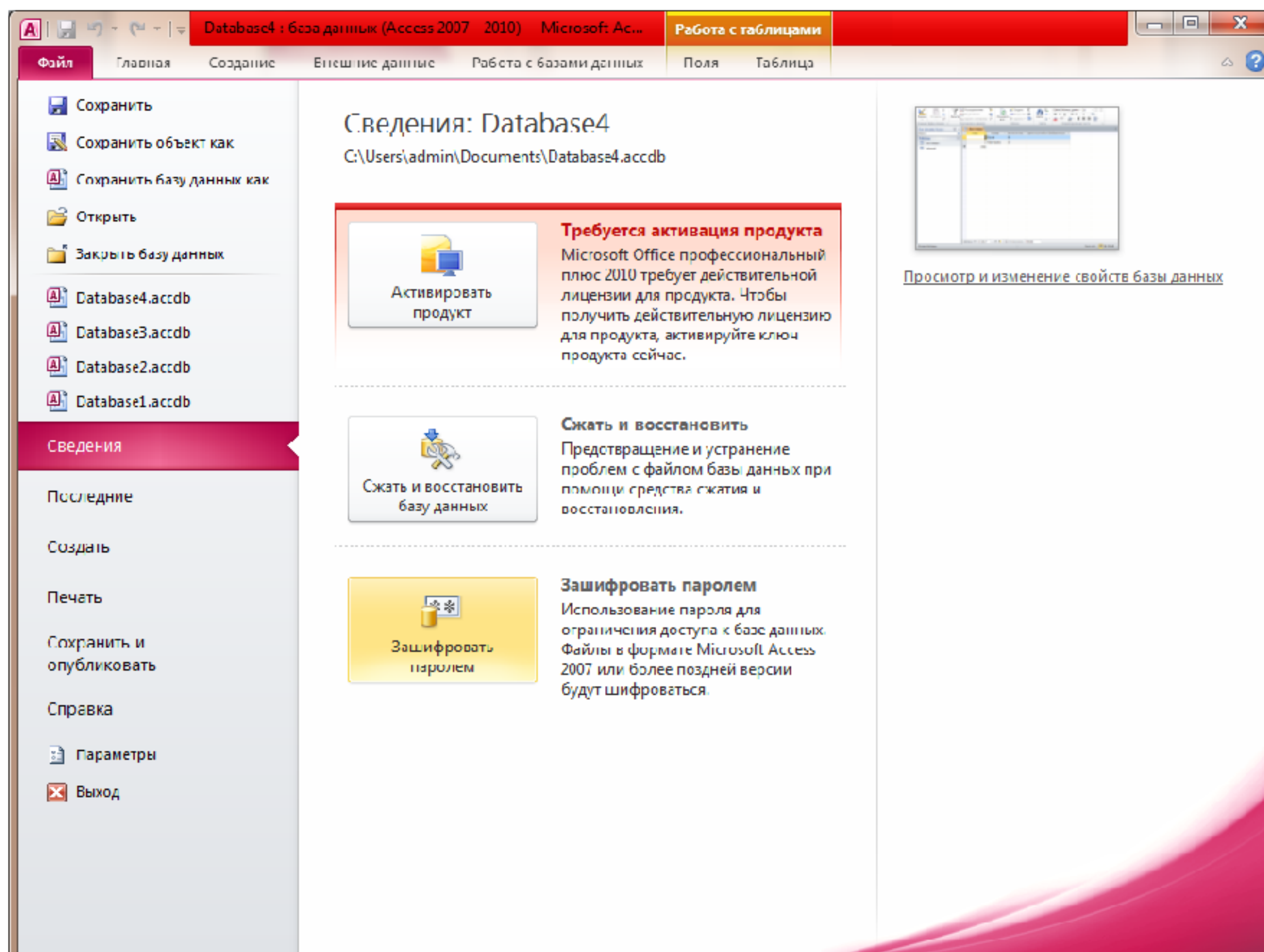
Для формирования базы данных «Персональный учет работников» используется табличная система управления базами данных Microsoft Access. Внутренняя «начинка» базы данных для ведения персонального учета работников в нашем примере будет состоять из следующих таблиц: «Карточки сотрудников», «Личные данные» 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.

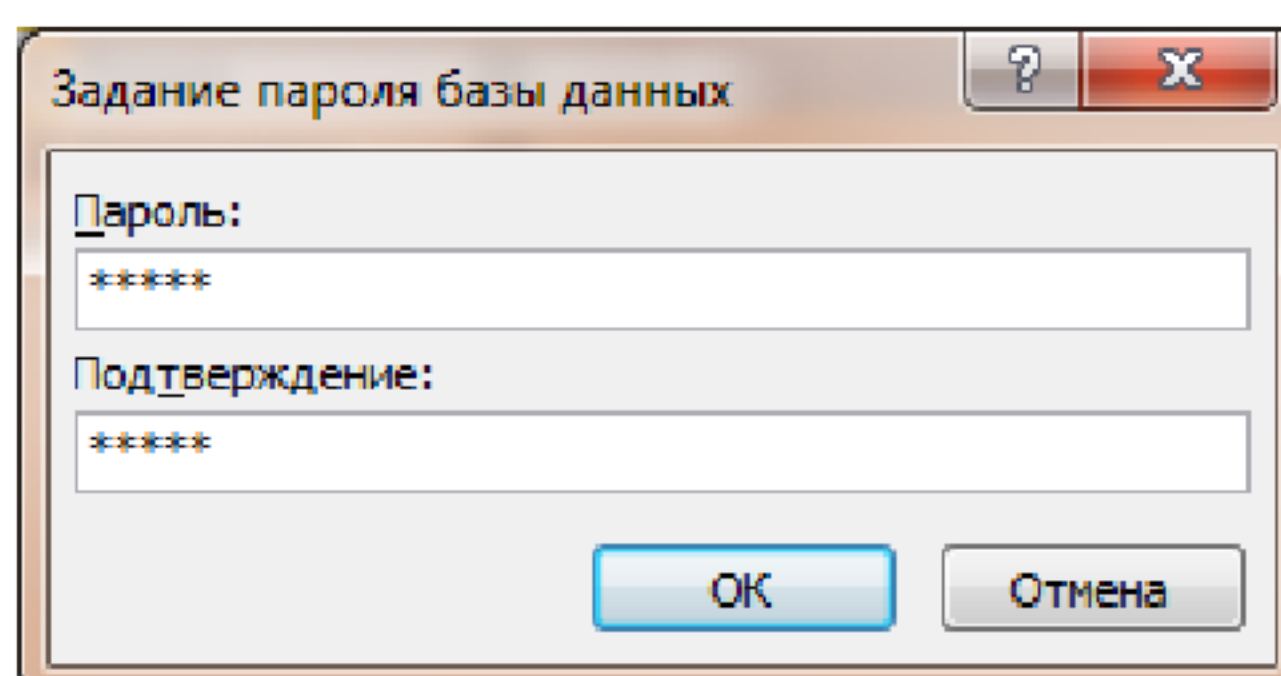


7. На вкладке Файл нажмите кнопку Сведения и выберите пункт Зашифровать паролем.

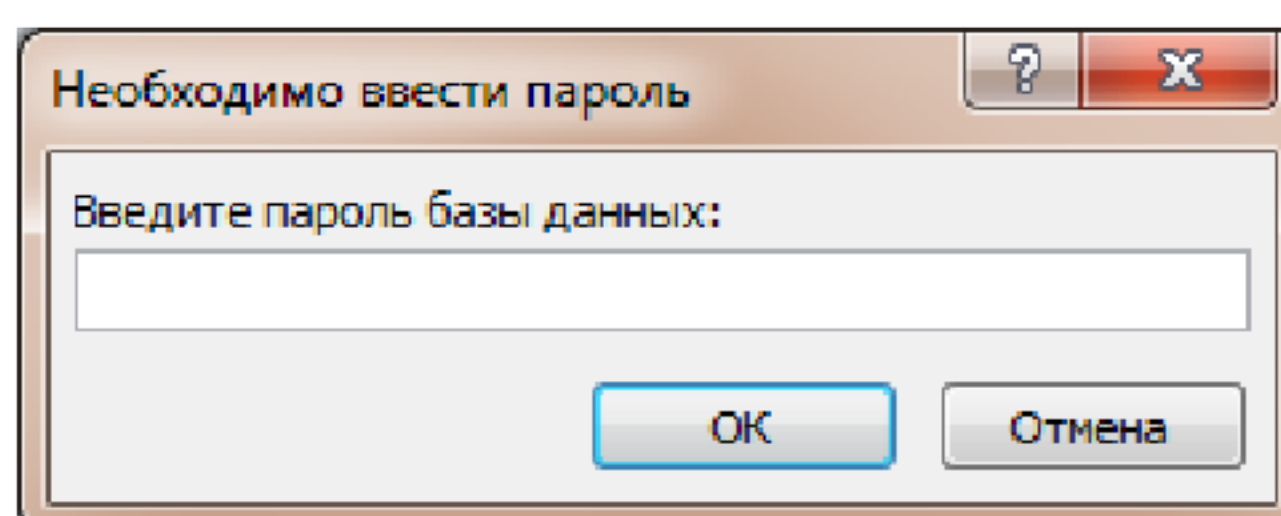




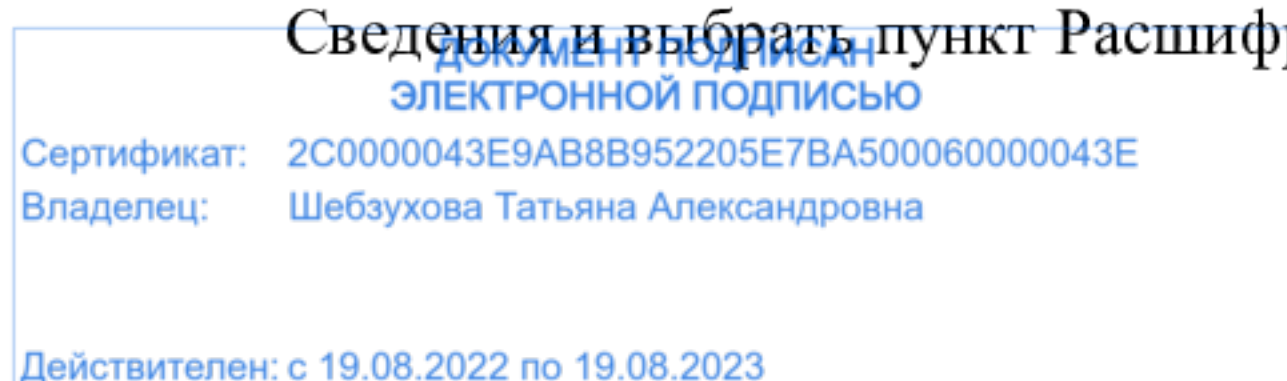
Откроется диалоговое окно Задание пароля базы данных. Введите пароль в поле Пароль, а затем повторите его в поле Проверить.

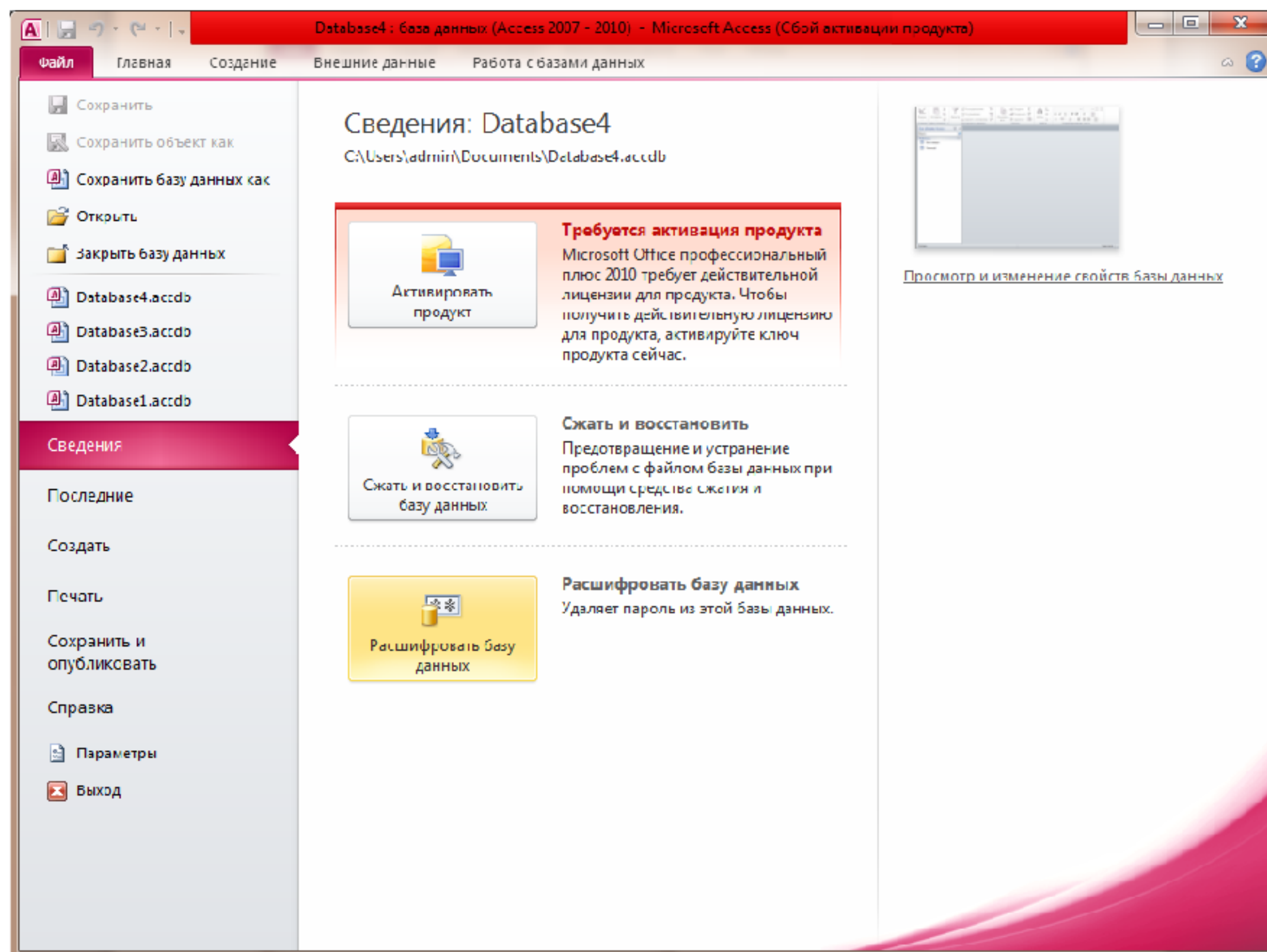


8. Закрывать БД.
9. Открыть защищенную паролем БД в монопольном режиме. Появится окно «Необходимо ввести пароль». Придумать и ввести пароль.

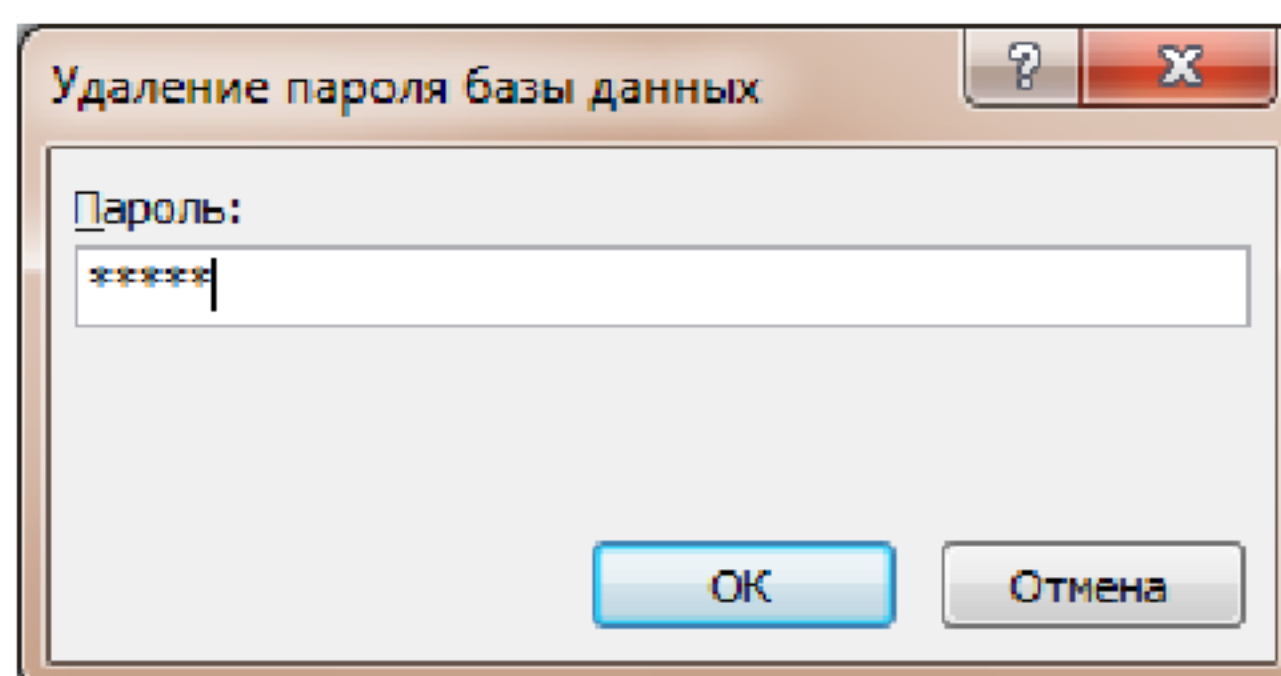


10. Для удаления созданного пароля необходимо зайти во вкладку Файл нажать кнопку Сведения и выбрать пункт Расшифровать базу данных.





Появится окно Удаления пароля баз данных.



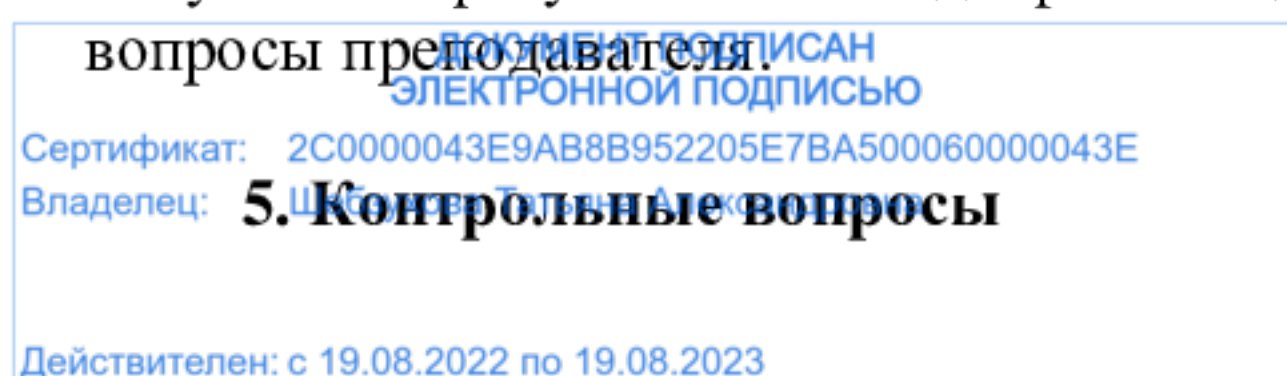
4. Содержание отчета:

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.

Защита 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.

Практическая работа №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.).

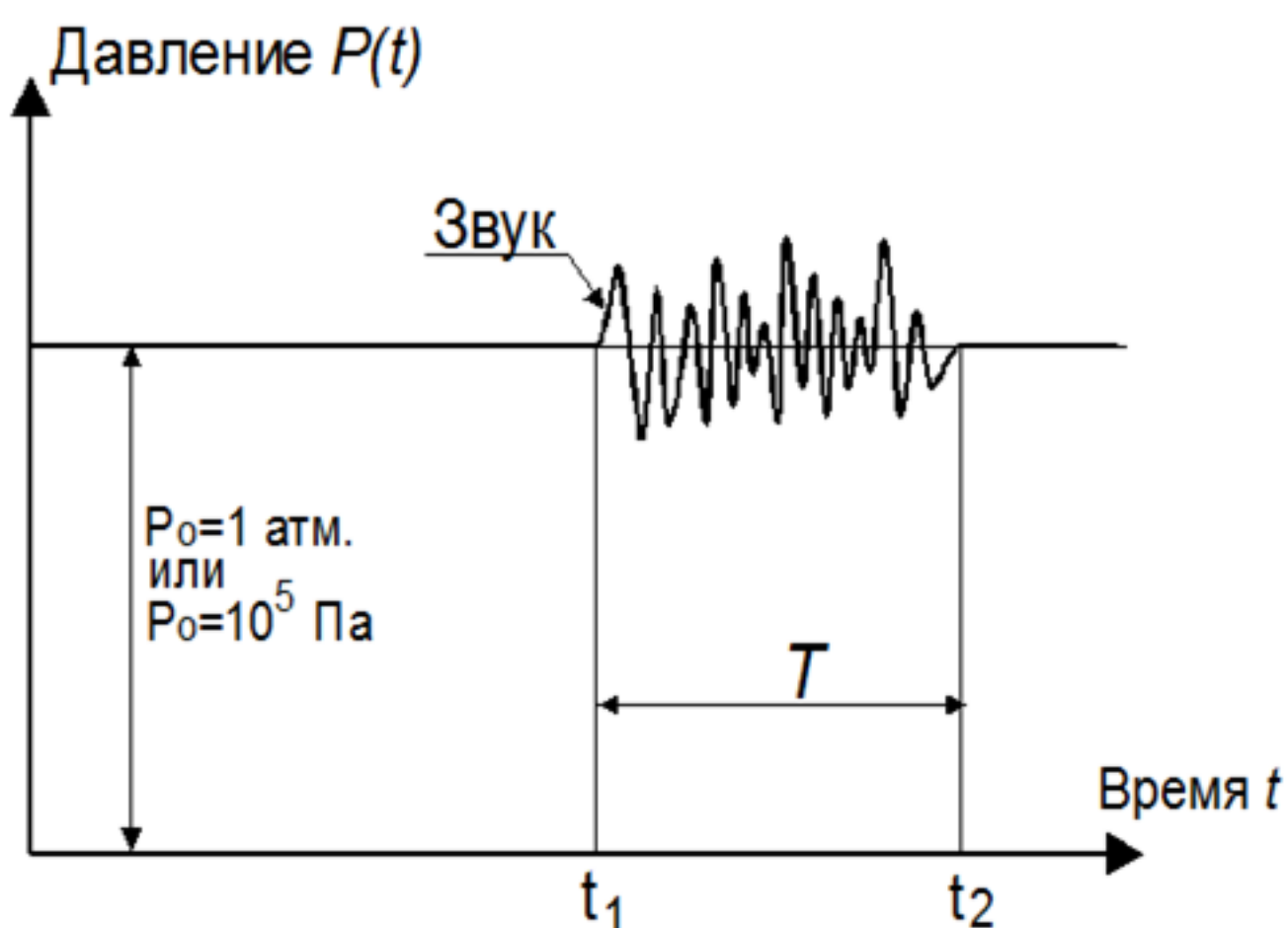


Рис.1. Изменение давление в воздушной среде при возникновении звука

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;

ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Исаева Татьяна Александровна
Действителен: с 19.08.2022 по 19.08.2023

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 $I_{над}$ 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:

$$\alpha_{пр} = I_{пр} / I_{над}$$

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

$$Q_{пер} = L_{над} - L_{пр} \quad , \text{откуда:}$$

$$L_{пр} = L_{над} - Q_{пер} \quad (1)$$

где:

$L_{над}$ — 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:

$$Q_{пер}(\text{дБ}) = 20 \lg \rho,$$

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:

$$2) Q_{пер}(\text{дБ}) = 12.5 \lg \rho + 14 - \text{ для стен с } \rho < 200 \text{ кг/м}^2 \quad (2)$$

$$3) Q_{пер}(\text{дБ}) = 14.5 \lg \rho + 15 - \text{ для стен с } \rho > 200 \text{ кг/м}^2 \quad (3)$$

$$4) Q_{пер}(\text{дБ}) = 14.3 \lg(\rho_1 + \rho_2) + 20 \lg \delta - 13 \quad (4)$$

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

где:

ρ_1 и ρ_2 — поверхностная плотность первой и второй перегородок,

δ

— толщина воздушного слоя между ними.

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

Случай использования неоднородной перегородки.

В качестве неоднородной ограждающей конструкции рассматриваются случаи:

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E

Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

- 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:

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

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/м ²	$Q_{пер}$, 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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Подпись: Александровна
Действителен: с 19.08.2022 по 19.08.2023

Керамзитобетонная плита	100,0	150,0	41,2
Керамзитобетонная плита	120,0	195,0	42,6
Шлакоблоки, оштукатуренные 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	3,0/3,0	-	32,0

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E

Владелец: ООО "Специальное строительство"

Действителен: с 19.08.2022 по 19.08.2023

(нар./внутр.)			
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, заполненная стекловатой:			
Без уплотняющих прокладок	-	-	30,0
С уплотняющими прокладками	-	-	33,0

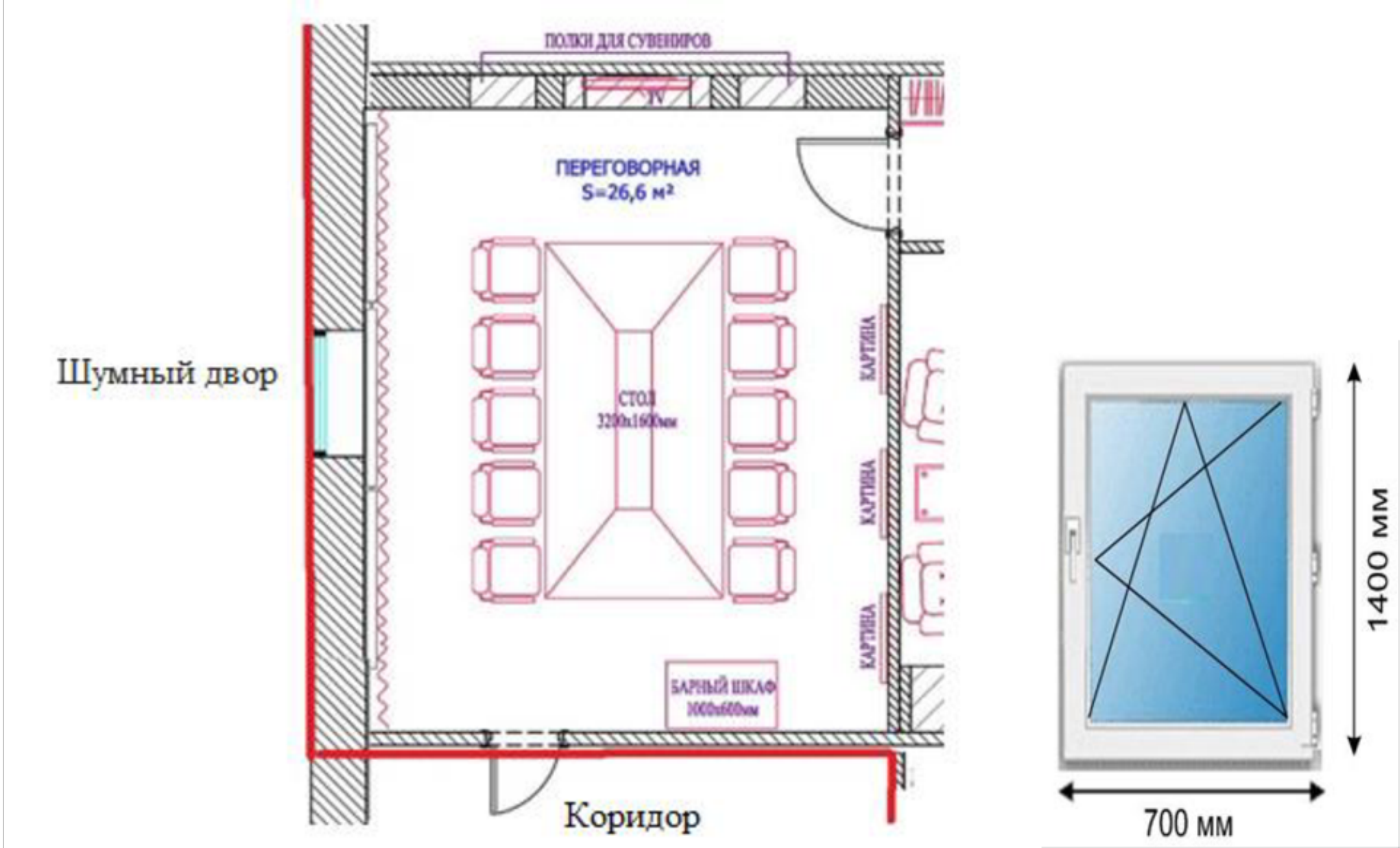
Сертификат: 2C00000043E9AB8B952205E7BA5000600000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

Щитовая дверь из твердых древесноволокнистых плит толщиной 4-6 мм с воздушным зазором 50 мм, заполненным минеральной ватой:			
Без уплотняющих прокладок	-	-	28,0
С уплотняющими прокладками	-	-	32,0
Тяжелая дубовая дверь размером 90x210 см, плотно пригнанная	-	-	25,0
Металлическая дверь (герметичная)	-	-	30,0

Пример расчёта

Рассмотрим возможность утечки речевых сообщений из исследуемого кабинета.



Размеры: 4x5м, h=3м.

Размер двери: 2x0,9м.

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 с коэффициентом звукоизоляции $Q_{per}=39,7$ дБ (табл. 1), дверь выходит в коридор.

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

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

Подставив соответствующие значения, получим:

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

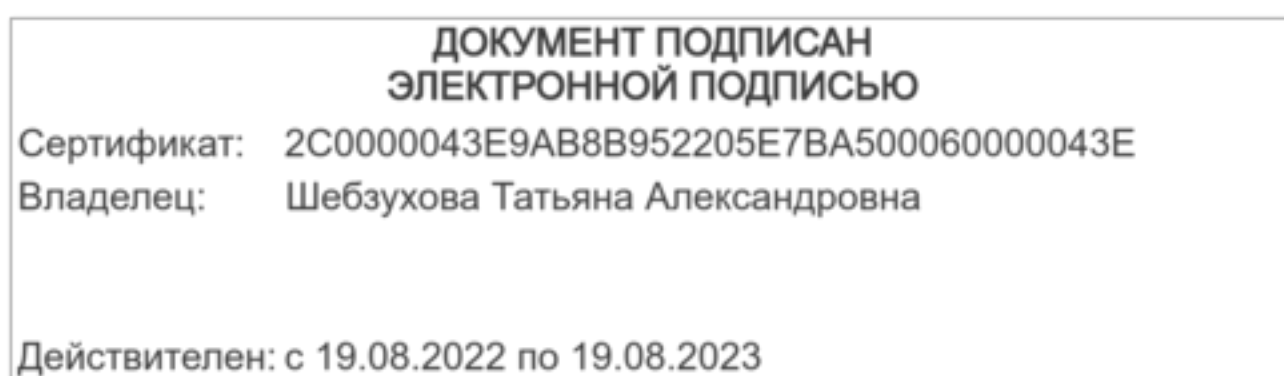
Защита отчета по лабораторной работе заключается в предъявлении преподавателю полученных результатов в виде файла и демонстрации полученных навыков при ответах на вопросы преподавателя.

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 $Q_{пер}$ 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).



Практическая работа №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_{np} 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_{np} примет следующий вид:

$$L_{np} = L_{nad} + 6 - Q_{пер} \quad (1)$$

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

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.

Документ подписан
Электронной подписью
Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна
Действителен: с 19.08.2022 по 19.08.2023

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_f определяют слоговую S , словесную W , фразовую разборчивость и понятность речи. Зависимость между формантной A_f (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_f определяется из выражения:

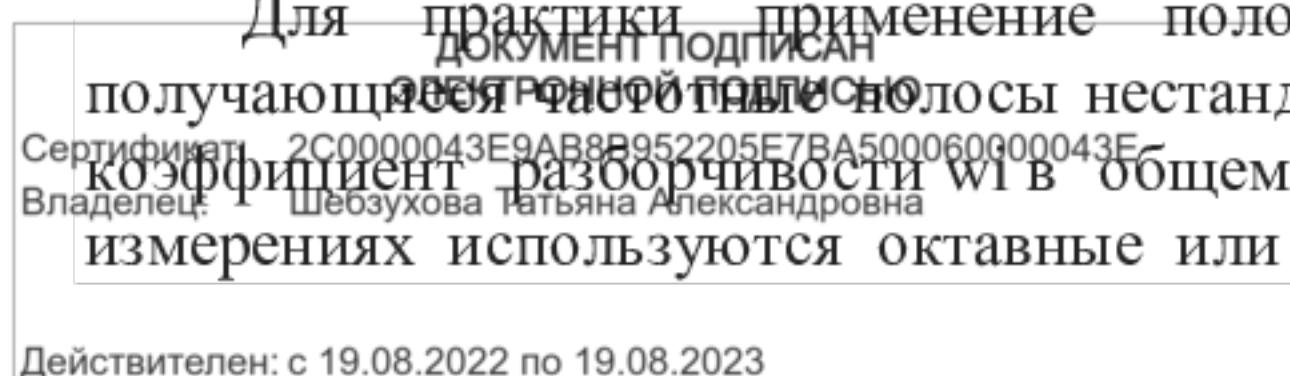
$$E_f = L_{np} - L_{ш}, \quad (1)$$

где:

$L_{ш}$ – уровень шума с внешней стороны перегородки;

L_{np} - 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 w 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_{ϕ} , 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

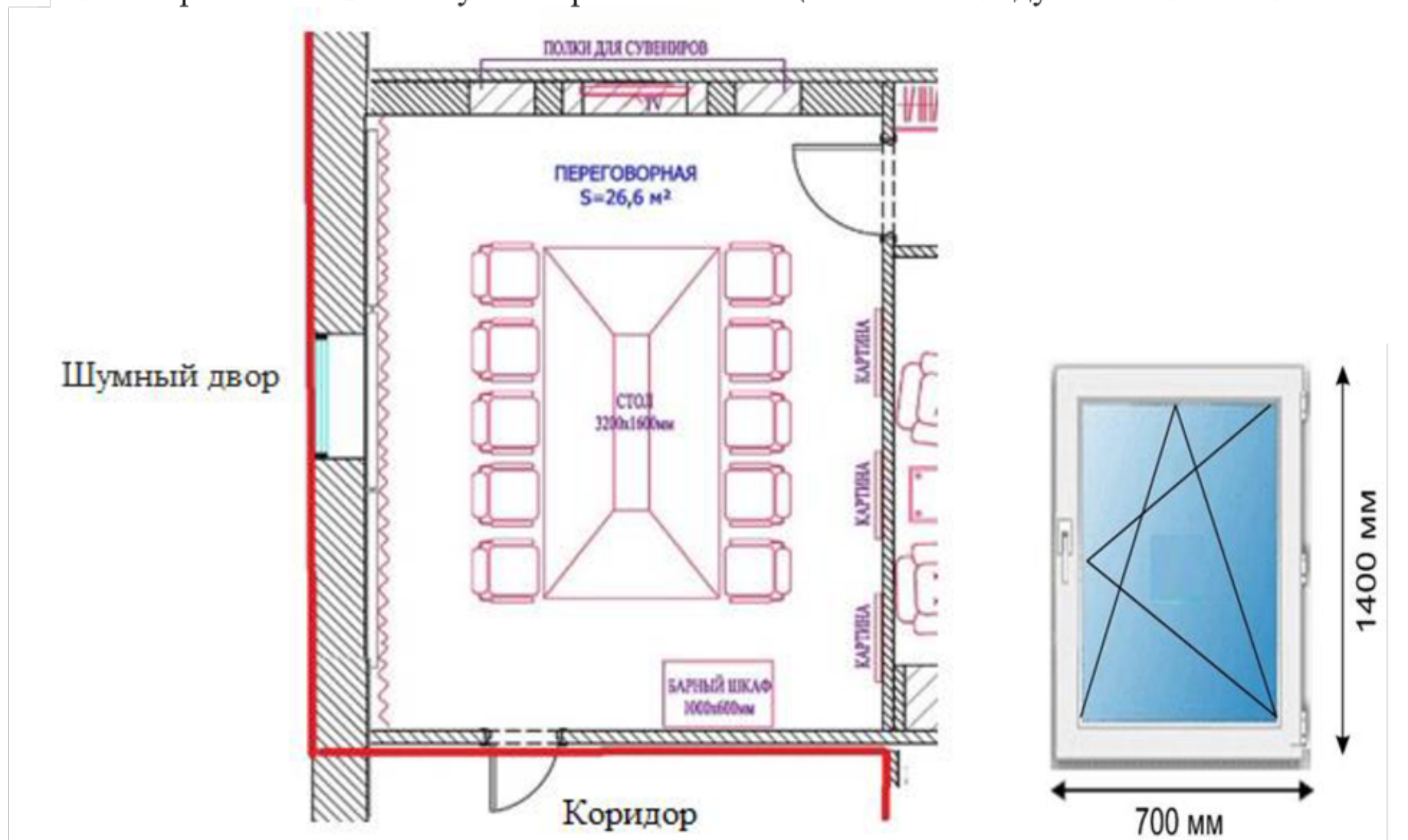
Понятность речи	Суммарная разборчивость формант A_{ϕ} , русск., %	Уровень ощущения формант E_{ϕ} , дБ
Смысл не понятен	<15	<-10
Предельно допустимая	15-22	-8...-10
Удовлетворительная	22-31	-6...-8
Хорошая	31-50	-3...-6
Отличная	=>50	=>-3

Обработка результатов.

На основании полученных результатов и рассчитанного уровня ощущения формант E_{ϕ} , дБ определяется суммарная разборчивость формант A_{ϕ} , 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 A_{ϕ} , русск., % установленного требованию защиты.

Пример расчёта

Рассмотрим возможность утечки речевых сообщений из исследуемого кабинета.



Размеры: 4x5м, h=3м.

Размер двери: 2x0,9м.

Документ подписан
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 2C0000043E9AB8B952205E7BA590060000043E
Владелец: Шебухова Татьяна Александровна

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

Действителен: с 19.08.2022 по 19.08.2023

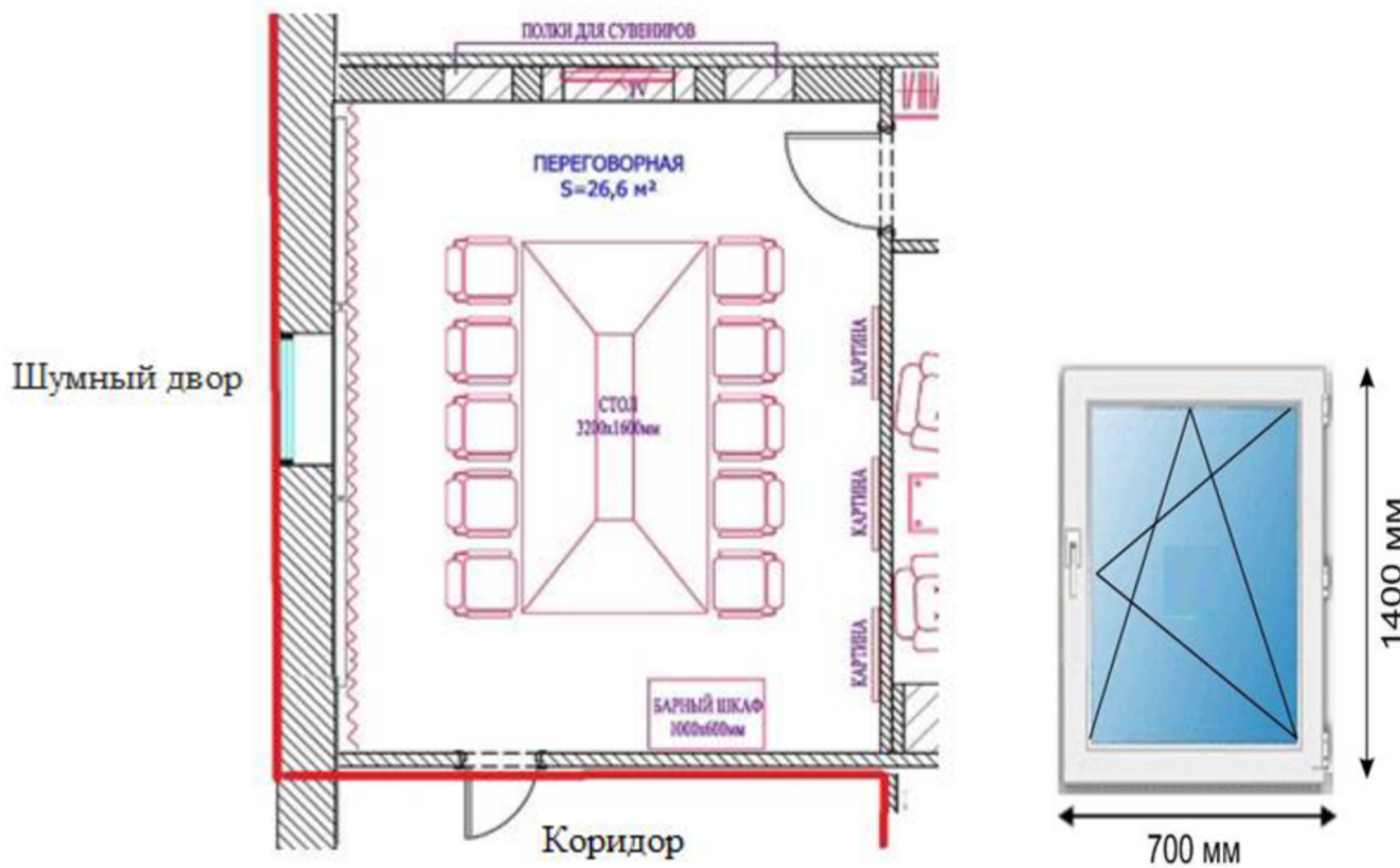
По формуле (1) определяем L_{np} (дБ). Значение L_{nad} - уровень речевого сигнала в контролируемом помещении, определяем по табл. 2 (выбираем максимальное значение диапазона). Источник звука – «Громкий»: 70 дБ.

В соответствии с выражением (1) определим уровни речевого сигнала за окном L_{np1} и за дверью L_{np2} :

$$L_{np1} = 70 + 6 - 39 = 37 \text{ дБ - за окном;}$$

$$L_{np2} = 70 + 6 - 25,7 = 51 \text{ дБ - за дверью в коридоре;}$$

Рассмотрим возможность утечки речевых сообщений из исследуемого кабинета.



Размеры: 4x5м, h=3м.

Размер двери: 2x0,9м.

Граница контролируемой зоны показана красным.

- $L_{np1} = 37$ дБ - за окном;
- $L_{np2} = 51$ 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 зависеть уровень шума, будем использовать наименьшее значение предельного спектра.

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

$$E_{\Phi1} = 37 - 45 = -8 \text{ дБ - за окном;}$$

$$E_{\Phi2} = 51 - 35 = 16 \text{ дБ - за дверью.}$$

В соответствии с данными табл. 2:

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

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E

Владелец: ООО «Техно-Электроника»

Действителен: с 19.08.2022 по 19.08.2023

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 A_{Φ} (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.

Защита 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 «Информационная безопасность в системе экономической безопасности»

Вариант № 1

Выполнил студент гр. _____

Проверил преподаватель
Мишин В.В.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

Пятигорск 2022

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.

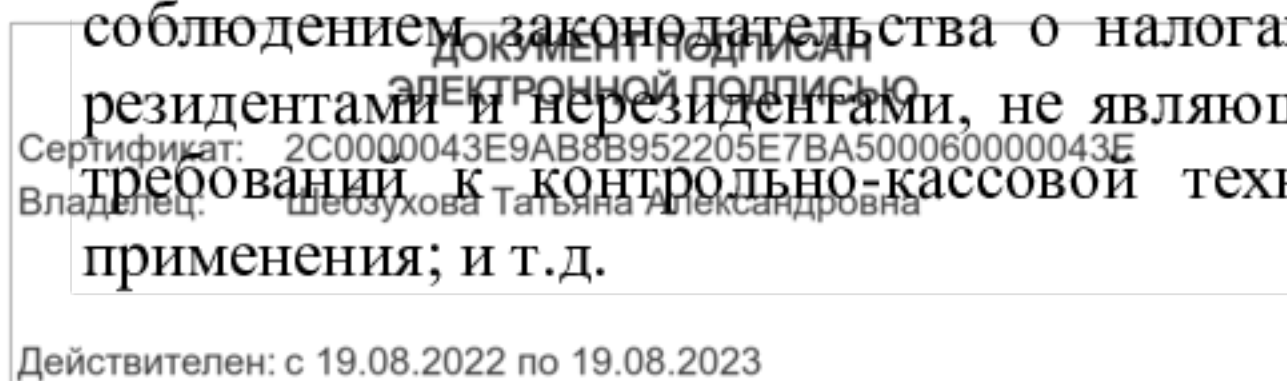
7. Предприятие «Астра». Основные функции предприятия: оказание консультационных услуг предприятиям, организациям, физическим лицам по широкому кругу вопросов экономики и права (создание и регистрация фирм, маркетинговые исследования, инновации, инвестиции, диагностика проблем клиентов и др.).

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.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ	
Сертификат:	2C0000043E9AB8B952205E7BA500060000043E
Владелец:	Шебзухова Татьяна Александровна
Действителен: с 19.08.2022 по 19.08.2023	

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:

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шибзухова Татьяна Александровна

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

Действителен: с 19.08.2022 по 19.08.2023

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;

Документ подписан
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна
Действителен: с 19.08.2022 по 19.08.2023

- «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

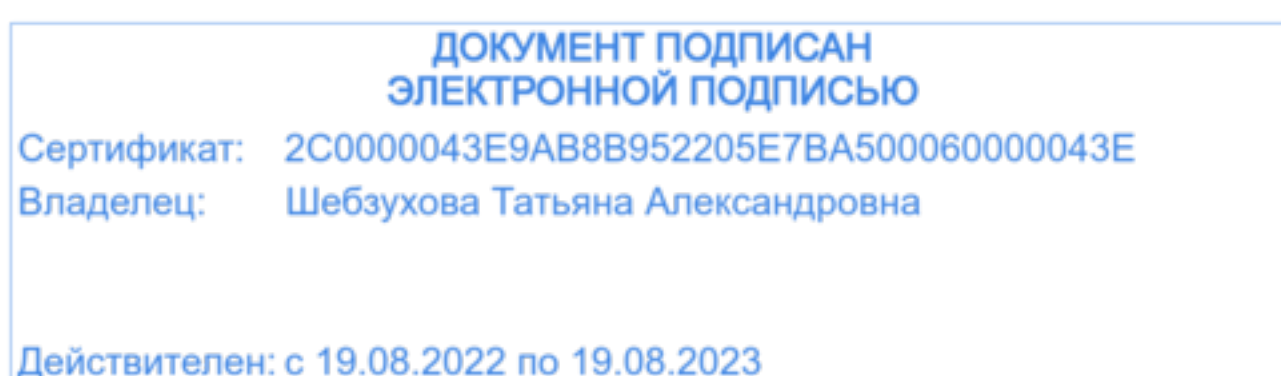
Ответственность за разработку мер и контроль обеспечения защиты информации несёт АИБ.

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:

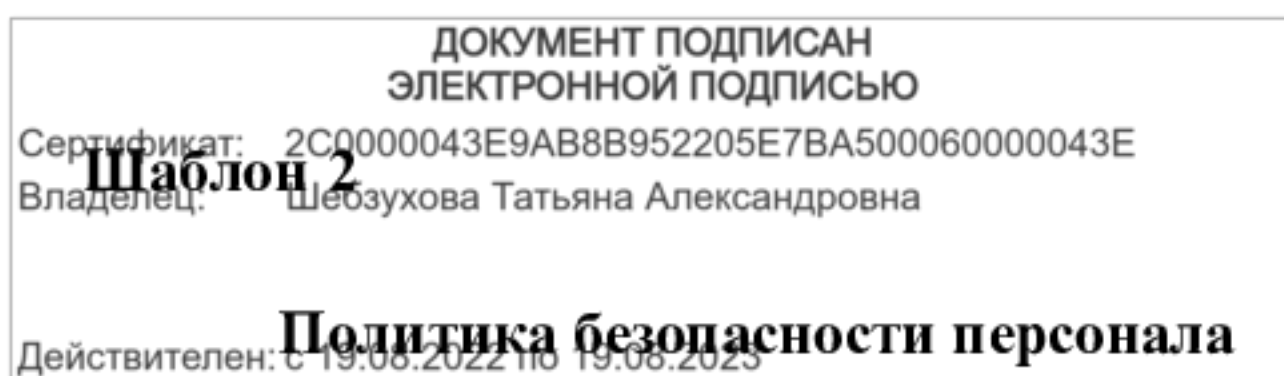
- применение соответствующих механизмов контроля для уменьшения величины риска до приемлемого уровня;
- сознательное и объективное принятие риска, если он точно удовлетворяет Политике Учреждения и критериям принятия рисков;
- уклонение от риска путём недопущения действий, могущих быть его причиной;
-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



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

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 00000000-00000000-00000000-00000000-00000000-00000000-00000000-00000000
Владелец: Шебзухова Татьяна Александровна
Действителен: с 19.08.2022 по 19.08.2023

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.

Сертификат:
Владелец:

2C0000043E9AB8B952205E7BA500060000043E
Пользователь: Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023