Автономная некоммерческая организация высшего образования
«Волгоградский институт бизнеса»

Рабочая программа учебной дисциплины

Информационная безопасность
(Наименование дисциплины)

09.03.03 Прикладная информатика, направленность (профиль) «Менеджмент в области информационных технологий
(Направление подготовки / Профиль)

Бакалавр
(Квалификация)

Кафедра разработчик Экономики и управления
Год набора **2023**

Вид учебной деятельности	Трудоемкость (объем) дисциплины					
	Очная форма	Очно-заочная форма		Заочная форма		
	д	в	св	з	сз	вв
Зачетные единицы	**4**			**4**	**4**	**4**
Общее количество часов	144			144	144	144
Аудиторные часы контактной работы обучающегося с преподавателями:	36			10	10	8
– Лекционные (Л)						
– Практические (ПЗ)	36			10	10	8
– *В том числе в форме практической подготовки*	*36*			*10*	*10*	*8*
– Лабораторные (ЛЗ)						
– Семинарские (СЗ)						
Самостоятельная работа обучающихся (СРО)	72			125	125	127
К (Р-Г) Р (П) (+;-)						
Тестирование (+;-)						
ДКР (+;-)						
Зачет (+;-)						
Зачет с оценкой (+;- (Кол-во часов))						
Экзамен (+;- (Кол-во часов))	+(36)			+ (9)	+ (9)	+ (9)

Волгоград 2023

Содержание

Раздел 1. Организационно-методический раздел

1.1. Цели освоения дисциплины

Дисциплина **«Информационная безопасность»** входит в **часть, формируемую участниками образовательных отношений** по направлению подготовки **«09.03.03 Прикладная информатика», направленность (профиль) «Менеджмент в области информационных технологий.**

Целью дисциплины является формирование **компетенций** (*в соответствии с ФГОС ВО и требованиями к результатам освоения основной профессиональной образовательной программы высшего образования (ОПОП ВО)*):

Универсальных:

УК-8.1. Способен обеспечивать безопасность на рабочем месте в условиях воздействия опасных производственных факторов, готов принимать участие в оказании первой помощи при травмах и внезапных заболеваниях

Общепрофессиональных:

ОПК-3.1 - Способен решать задачи, связанные с обеспечением информационной безопасности

Перечисленные компетенции формируются в процессе достижения **индикаторов компетенций:**

Обобщенная трудовая функция/ трудовая функция	**Код и наименование дескриптора компетенций**	**Код и наименование индикатора достижения компетенций (из ПС)**
ПС 06.012 Менеджер продуктов в области информационных технологий **С Управление серией ИТ-продуктов и группой их менеджеров** **С/05.6** Командообразование и развитие персонала **С/09.6** Разработка предложений п приобретению и продаже технологических, продуктовых и прочих интеллектуальных активов и организаций	УК-8.1. Способен обеспечивать безопасность на рабочем месте в условиях воздействия опасных производственных факторов, готов принимать участие в оказании первой помощи при травмах и внезапных заболеваниях	*Знает* ИД-1 УК- 8.1 Основы защиты интеллектуальной собственности С/09.6 *Умеет* ИД-3 УК- 8.1 Проводить переговоры с командой менеджеров ИТ-продуктов С/05.6 *Имеет навыки и (или) опыт:* ИД-5 УК- 8.1 Наставничество и коучинг, включая организацию обучения персонала С/05.6
ПС 06.012 Менеджер продуктов в области информационных технологий **С Управление серией ИТ-продуктов и группой их менеджеров** **С/09.6** Разработка предложений п приобретению и продаже технологических, продуктовых и прочих интеллектуальных активов и организаций	ОПК-3.1 - Способен решать задачи, связанные с обеспечением информационной безопасности	*Знает:* ИД-1 ОПК- 3.1 Основы защиты интеллектуальной собственности С/09.6 *Умеет:* ИД-3 ОПК- 3.1 Проводить оценку ценности технологий, ИТ-продуктов и организаций как потенциальных активов для приобретения с целью развития серии ИТ-продуктов С/09.6 *Имеет навыки и (или) опыт:* ИД-5 ОПК- 3.1 Исследование существующих на рынке технологий, ИТ-продуктов и организаций как потенциальных активов для приобретения с целью

		развития серии ИТ-продуктов С/09.6

1.2. Место дисциплины в структуре ОПОП ВО направления подготовки «09.03.03 Прикладная информатика», направленность (профиль) «Менеджмент в области информационных технологий

№	Предшествующие дисциплины (дисциплины, изучаемые параллельно)	Последующие дисциплины
1	*2*	*3*
1	Введение в направление подготовки	ВКР
2	Информатика	
3	Правовые основы прикладной информатики	
4	Информационные системы и технологии	
5	Информационные технологии в менеджменте	
6	Базы данных	
7	Вычислительные системы, сети и телекоммуникации	
8	Проектный практикум	
9	Проектирование веб-сайтов	

Последовательность формирования компетенций в указанных дисциплинах может быть изменена в зависимости от формы и срока обучения, а также преподавания с использованием дистанционных технологий обучения.

1.3. Нормативная документация

Рабочая программа учебной дисциплины составлена на основе:

- Федерального государственного образовательного стандарта высшего образования по направлению подготовки **09.03.03 Прикладная информатика**;
- учебного плана направления подготовки **09.03.03 Прикладная информатика, направленность (профиль) «Менеджмент в области информационных технологий»** 2023 года набора;
- образца рабочей программы учебной дисциплины (приказ № 113-О от 01.09.2021 г.).

Раздел 2. Тематический план

Очная форма обучения (полный срок)

№	Тема дисциплины	Трудоемкость					
		Всего	Аудиторные занятия			СРО	Код индикатора и дескриптора достижения компетенций
			Л	ПЗ (ЛЗ, СЗ)	Прак. Подг.		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	Понятие информационной безопасности. Основные составляющие.	8				8	ИД-1 УК- 8.1 ИД-1 ОПК- 3.1
2	Угрозы информационной безопасности. Их классификация	8				8	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	14		4	4	10	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
4	Административный уровень. Политика безопасности	8				8	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
5	Организация разноуровневого доступа в информационную систему	12		4	4	8	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
6	Основные программно-технические меры. Защита информации с помощью пароля	14		8	8	6	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
7	Защита от несанкционированного доступа и сетевых хакерских атак	10		4	4	6	ИД-1 УК- 8.1 ИД-5 ОПК- 3.1
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	16		8	8	8	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
9	Основы технологии построения защищенных ОС	18		8	8	10	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
Вид промежуточной аттестации (экзамен)		**36**					
Итого		**108**		**36**	**36**	**72**	

Заочная форма обучения (полный срок, ускоренное обучение на базе СПО)

№	Тема дисциплины	Трудоемкость					
		Всего	Аудиторные занятия			СРО	Код индикатора и дескриптора достижения компетенций
			Л	ПЗ (ЛЗ, СЗ)	Прак. Подг.		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	Понятие информационной безопасности. Основные составляющие. Важность	14				14	ИД-1 УК- 8.1 ИД-1 ОПК- 3.1

	проблемы						
2	Угрозы информационной безопасности. Их классификация	14				14	ИД-3 УК- 8.1 ИД-5 ОПК-3.1
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	16		2	2	14	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
4	Административный уровень. Политика безопасности	14				14	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
5	Организация разноуровневого доступа в информационную систему	18		2	2	16	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
6	Основные программно-технические меры. Защита информации с помощью пароля	17		2	2	15	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
7	Защита от несанкционированного доступа и сетевых хакерских атак	12				12	ИД-1 УК- 8.1 ИД-5 ОПК- 3.1
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	14		2	2	12	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
9	Основы технологии построения защищенных ОС	16		2	2	14	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
Вид промежуточной аттестации (экзамен)		**9**					
Итого		**144**		**10**	**10**	**125**	

Заочная форма обучения (ускоренное обучение на базе ВО)

№	Тема дисциплины	Трудоемкость					
		Всего	Аудиторные занятия			СРО	Код индикатора и дескриптора достижения компетенций
			Л	ПЗ (ЛЗ, СЗ)	Прак. Подг.		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*
1	Понятие информационной безопасности. Основные составляющие. Важность проблемы	14				14	ИД-1 УК- 8.1 ИД-1 ОПК- 3.1
2	Угрозы информационной безопасности. Их классификация	14				14	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	16		2	2	14	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
4	Административный уровень. Политика безопасности	14				14	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
5	Организация разноуровневого доступа в информационную систему	18		2	2	16	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
6	Основные программно-технические меры. Защита информации с помощью пароля	17		2	2	15	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1

7	Защита от несанкционированного доступа и сетевых хакерских атак	14				14	ИД-1 УК- 8.1 ИД-5 ОПК- 3.1
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	14				12	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
9	Основы технологии построения защищенных ОС	16		2	2	14	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
Вид промежуточной аттестации (экзамен)		**9**					
Итого		**144**		**8**	**8**	**127**	

Раздел 3. Содержание дисциплины

3.1. Содержание дисциплины

Тема 1. Понятие информационной безопасности. Основные составляющие. Важность проблемы

Организация ИТ-инфраструктуры и управление информационной безопасностью. Информационная безопасность – защита интересов субъектов информационных отношений. Доктрина информационной безопасности РФ. Доступность, целостность и конфиденциальность информации. Предмет и объект защиты. Информационная безопасность один из важнейших аспектов интегральной безопасности.

Тема 2. Угрозы информационной безопасности. Их классификация

Информационная безопасность, как часть эксплуатации современных информационных систем. Угроза. Угроза информационной безопасности. Утечка информации. Наиболее распространенные угрозы доступности. Примеры угроз доступности. Основные угрозы целостности. Основные угрозы конфиденциальности. Классификация угроз по основным признакам.

Тема 3. Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства

Важность законодательного уровня информационной безопасности. Обзор российского законодательства в области информационной безопасности. Закон «Об информации, информационных технологиях и защите информации». Другие законы и нормативные акты федеральной службы экспертного и технического контроля (гостехкомиссии). Обзор зарубежного законодательства в области информационной безопасности. О текущем состоянии российского законодательства в области информационной безопасности.

Тема 4. Административный уровень. Политика безопасности

Управление информационной безопасностью. Политика безопасности. Программа безопасности. Синхронизация программы безопасности с жизненным циклом.

Тема 5. Организация разноуровневого доступа в информационную систему

Типы политик безопасности. Ролевое управление доступом.

Тема 6. Основные программно-технические меры. Защита информации с помощью пароля

Основные понятия программно-технического уровня информационной безопасности. Особенности современных информационных систем, существенные с точки зрения безопасности. Архитектурная безопасность. Идентификация и аутентификация. Парольная аутентификация. Одноразовые пароли. Идентификация / аутентификация с помощью биометрических данных.

Тема 7. Защита от несанкционированного доступа и сетевых хакерских атак

Противодействие несанкционированному доступу. Способы несанкционированного доступа. Методы и средства борьбы с несанкционированным доступом.

Тема 8. Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов

Программы обнаружения и защиты от вирусов. Программы-доктора. Программы-детекторы. Программы-мониторы и др. Обзор антивирусного программного обеспечения. Информационная инфекция. Вирус. Резидентные вирусы. Полиморфизм. Троянские кони. Сетевые черви. Классификация компьютерных вирусов.

Тема 9. Основы технологии построения защищенных ОС

Подходы к обеспечению безопасности ОС. Задачи разработки защищенных ОС. Проблема внедрения модели безопасности в ОС. Критика внедрения моделей. Постановка задачи внедрения модели безопасности в ОС. Решение проблемы внедрения моделей безопасности в ОС.

3.2. Содержание практического блока дисциплины

Очная форма обучения (полный срок)

№	Тема практического (семинарского, практического) занятия *В том числе в форме практической подготовки*
1	***2***
Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	
ПЗ 1	Изучение нормативно – правовой базы в области информационной безопасности
Организация разноуровневого доступа в информационную систему	
ПЗ 2	Администрирование баз данных и проектов Access
Основные программно-технические меры. Защита информации с помощью пароля	
ПЗ 3	Создание резервных копий файлов (для баз данных и проектов Access)
ПЗ 4	Защита информации с помощью пароля
Защита от несанкционированного доступа и сетевых хакерских атак	
ПЗ 5	Защита от несанкционированного доступа и сетевых хакерских атак
Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	
ПЗ 6	Защита съемных устройств с помощью современного антивирусного программного обеспечения
ПЗ 7	Настройка антивирусной системы безопасности
Основы технологии построения защищенных ОС	
ПЗ 8	Основные признаки присутствия на компьютере вредоносных программ
ПЗ 9	Общие требования к построению системы безопасности

Заочная форма обучения (полный срок, ускоренное обучение на базе СПО)

№	Тема практического (семинарского, практического) занятия *В том числе в форме практической подготовки*
1	***2***
Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	
ПЗ 1	Изучение нормативно – правовой базы в области информационной безопасности
Организация разноуровневого доступа в информационную систему	
ПЗ 2	Администрирование баз данных и проектов Access
Основные программно-технические меры. Защита информации с помощью пароля	
ПЗ 3	Создание резервных копий файлов (для баз данных и проектов Access)
Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	
ПЗ 4	Защита съемных устройств с помощью современного антивирусного программного обеспечения
Основы технологии построения защищенных ОС	
ПЗ 5	Основные признаки присутствия на компьютере вредоносных программ

Заочная форма обучения (ускоренное обучение на базе ВО)

№	Тема практического (семинарского, практического) занятия *В том числе в форме практической подготовки*
1	***2***
Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	
ПЗ 1	Изучение нормативно – правовой базы в области информационной безопасности
Организация разноуровневого доступа в информационную систему	
ПЗ 2	Администрирование баз данных и проектов Access
Основные программно-технические меры. Защита информации с помощью пароля	
ПЗ 3	Создание резервных копий файлов (для баз данных и проектов Access)
Основы технологии построения защищенных ОС	
ПЗ 4	Основные признаки присутствия на компьютере вредоносных программ

3.3. Образовательные технологии

Очная форма обучения (полный срок)

№	Тема занятия	Вид учебного занятия	Форма / Методы интерактивного обучения	% учебного времени
1	***2***	***3***	***4***	***5***
1	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	ПЗ	Дискуссия	25
2	Организация разноуровневого доступа в информационную систему	ПЗ	Деловая игра	25
3	Основные программно-технические меры. Защита информации с помощью пароля	ПЗ	Мозговой штурм	25
4	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	ПЗ	Конференция	25
5	Основы технологии построения защищенных ОС	ПЗ	Дискуссия	25
Итого				**25%**

Заочная форма обучения (полный срок, ускоренное обучение на базе СПО)

№	Тема занятия	Вид учебного занятия	Форма / Методы интерактивного обучения	% учебного времени
1	***2***	***3***	***4***	***5***
1	Основные программно-технические меры. Защита информации с помощью пароля	ПЗ	Мозговой штурм	25
2	Современные антивирусные программы. Защита от	ПЗ	Конференция	25

	информационных инфекций. Классификация компьютерных вирусов			
3	Основы технологии построения защищенных ОС	ПЗ	Дискуссия	25
Итого				**25%**

Заочная форма обучения (ускоренное обучение на базе ВО)

№	**Тема занятия**	**Вид учебного занятия**	**Форма / Методы интерактивного обучения**	**% учебного времени**
1	***2***	***3***	***4***	***5***
1	Основные программно-технические меры. Защита информации с помощью пароля	ПЗ	Мозговой штурм	25
3	Основы технологии построения защищенных ОС	ПЗ	Дискуссия	25
Итого				**25%**

Раздел 4. Организация самостоятельной работы обучающихся

4.1. Организация самостоятельной работы обучающихся

№	Тема дисциплины	№ вопросов	№ рекомендуемой литературы
1	*2*	*3*	*4*
1	Понятие информационной безопасности. Основные составляющие. Важность проблемы	1,2,3	3, 6, 7
2	Угрозы информационной безопасности. Их классификация	2,3	1, 2, 3, 4
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства	4,5,6,7,8,9,10	2, 3, 4
4	Административный уровень. Политика безопасности	11,12,17,18,19	1, 3, 4
5	Организация разноуровневого доступа в информационную систему	20,21	1, 3, 4
6	Основные программно-технические меры. Защита информации с помощью пароля	13,14	3, 6, 7
7	Защита от несанкционированного доступа и сетевых хакерских атак	17,18,19.20,21	3, 6, 7
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов	15,16,19,22	3, 6, 7
9	Основы технологии построения защищенных ОС	17,18,19,20,21	3, 6, 7

Перечень вопросов, выносимых на самостоятельную работу обучающихся

1. Подходы к изучению информационной безопасности
2. Моделирование информационной безопасности
3. Причины, виды и каналы утечки информации
4. Закон «Об информации, информационных технологиях и защите информации».
5. Зарубежное законодательство в области информационной безопасности.
6. Роль стандартов информационной безопасности.
7. Стандарты ISO 17799 и ISO/IEC 15408 «Критерии оценки безопасности информационных технологий».
8. Функциональные требования. Требования доверия безопасности.
9. Гармонизированные критерии Европейских стран.
10. Спецификации в области информационной безопасности.
11. Политика безопасности. Типы политик безопасности
12. Программа безопасности
13. Основные классы мер процедурного уровня
14. Архитектурная безопасность
15. Отказоустойчивость и зона риска. Обеспечение отказоустойчивости.
16. Туннелирование и управление.
17. Мотивация как лояльность персонала с точки зрения информационной безопасности.
18. Человеческий фактор в обеспечении безопасности конфиденциальной информации
19. Особенности современных информационных систем, существенные с точки зрения безопасности.
20. Анализ и классификация удаленных атак на компьютерные сети
21. Многоуровневая защита корпоративных сетей
22. Современное антивирусное программное обеспечение

4.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся

Самостоятельная работа обучающихся обеспечивается следующими учебно-методическими материалами:

1. Указаниями в рабочей программе по дисциплине (п.4.1.)
2. Лекционными материалами в составе учебно-методического комплекса по дисциплине
3. Заданиями и методическими рекомендациями по организации самостоятельной работы обучающихся в составе учебно-методического комплекса по дисциплине.
4. Глоссарием по дисциплине в составе учебно-методического комплекса по дисциплине.

Раздел 5. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся

Фонд оценочных средств по дисциплине представляет собой совокупность контролирующих материалов, предназначенных для измерения уровня достижения обучающимися установленных результатов образовательной программы. ФОС по дисциплине используется при проведении оперативного контроля и промежуточной аттестации обучающихся. Требования к структуре и содержанию ФОС дисциплины регламентируются Положением о фонде оценочных материалов по программам высшего образования – программам бакалавриата, магистратуры.

5.1. Паспорт фонда оценочных средств

Очная форма обучения (полный срок)

№	Контролируемые разделы (темы) дисциплины	Оценочные средства				
		Л	ПЗ (ЛЗ, СЗ)	Прак. Подг.	СРО	Код индикатора и дескриптора достижения компетенций
1	*2*	*3*	*4*	*5*	*6*	*7*
1	Понятие информационной безопасности. Основные составляющие. Важность проблемы				ПРВ	ИД-1 УК- 8.1 ИД-1 ОПК- 3.1
2	Угрозы информационной безопасности. Их классификация				ПРВ	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства		УО	УО	ПРВ	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
4	Административный уровень. Политика безопасности				ПРВ	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
5	Организация разноуровневого доступа в информационную систему		УО	УО	ПРВ	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
6	Основные программно-технические меры. Защита информации с помощью пароля		МШ	МШ	ПРВ	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
7	Защита от несанкционированного доступа и сетевых хакерских атак		УО	УО	ПРВ	ИД-1 УК- 8.1 ИД-5 ОПК- 3.1
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов		УО	УО	ПРВ	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
9	Основы технологии построения защищенных ОС		Д	Д	ПРВ	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1

Заочная форма обучения (полный срок, ускоренное обучение на базе СПО)

№	Контролируемые разделы (темы) дисциплины	Оценочные средства				
		Л	ПЗ (ЛЗ, СЗ)	Прак. Подг.	СРО	Код индикатора и дескриптора достижения компетенций
1	*2*	*3*	*4*	*5*	*6*	*7*
1	Понятие информационной безопасности. Основные составляющие. Важность проблемы				ПРВ	ИД-1 УК- 8.1 ИД-1 ОПК- 3.1
2	Угрозы информационной безопасности. Их классификация				ПРВ	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства		УО	УО	ПРВ	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
4	Административный уровень. Политика безопасности				ПРВ	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
5	Организация разноуровневого доступа в информационную систему		УО	УО	ПРВ	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
6	Основные программно-технические меры. Защита информации с помощью пароля		МШ	МШ	ПРВ	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
7	Защита от несанкционированного доступа и сетевых хакерских атак				ПРВ	ИД-1 УК- 8.1 ИД-5 ОПК- 3.1
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов				ПРВ	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
9	Основы технологии построения защищенных ОС		Д	Д	ПРВ	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1

Заочная форма обучения (ускоренное обучение на базе ВО)

№	Контролируемые разделы (темы) дисциплины	Оценочные средства				
		Л	ПЗ (ЛЗ, СЗ)	Прак. Подг.	СРО	Код индикатора и дескриптора достижения компетенций
1	*2*	*3*	*4*		*5*	*6*
1	Понятие информационной безопасности. Основные составляющие. Важность проблемы				ПРВ	ИД-1 УК- 8.1 ИД-1 ОПК- 3.1

2	Угрозы информационной безопасности. Их классификация				ПРВ	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
3	Законодательный уровень информационной безопасности: обзор российского и зарубежного законодательства		УО	УО	ПРВ	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
4	Административный уровень. Политика безопасности				ПРВ	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
5	Организация разноуровневого доступа в информационную систему		УО	УО	ПРВ	ИД-3 УК- 8.1 ИД-1 ОПК- 3.1
6	Основные программно-технические меры. Защита информации с помощью пароля		МШ	МШ	ПРВ	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1
7	Защита от несанкционированного доступа и сетевых хакерских атак				ПРВ	ИД-1 УК- 8.1 ИД-5 ОПК- 3.1
8	Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов				ПРВ	ИД-3 УК- 8.1 ИД-5 ОПК- 3.1
9	Основы технологии построения защищенных ОС		Д	Д	ПРВ	ИД-5 УК- 8.1 ИД-3 ОПК- 3.1

Условные обозначения оценочных средств (Столбцы 3, 4, 5):
ЗЗ – Защита выполненных заданий (творческих, расчетных и т.д.), представление презентаций;
Т – Тестирование по безмашинной технологии;
АСТ – Тестирование компьютерное;
УО – Устный (фронтальный, индивидуальный, комбинированный) опрос;
КР – Контрольная работа (аудиторные или домашние, индивидуальные, парные или групповые контрольные, самостоятельные работы, диктанты и т.д.);
К – Коллоквиум;
ПРВ – Проверка рефератов, отчетов, рецензий, аннотаций, конспектов, графического материала, эссе, переводов, решений заданий, выполненных заданий в электронном виде и т.д.;
ДИ – Деловая игра;
РИ – Ролевая игра;
КМ – Кейс-метод;
КС – Круглый стол;
КСМ – Компьютерная симуляция;
МШ – Метод мозгового штурма;
ЛС – Лекция-ситуация;
ЛК – Лекция-конференция;
ЛВ – Лекция-визуализация;
ПЛ – Проблемная лекция;
Д – Дискуссия, полемика, диспут, дебаты;
П – Портфолио;
ПВУ – Просмотр видеоуроков;
МП – Метод проектов.

5.2. Оценочные средства текущего контроля
Перечень практических (семинарских) заданий

Тема № 5: «Организация разноуровневого доступа в информационную систему»

Практическая работа. Администрирование баз данных и проектов Access

Цель - изучить способы защиты информации в базе данных Access от несанкционированного доступа.

Результат обучения. После обучения студент должен:
- знать способы защиты информации в СУБД Access;
- уметь осуществлять настройку системы безопасности СУБД Access на трех уровнях.

Администрирование защищенных баз данных и проектов Access

Существует несколько способов защиты базы данных Access от несанкционированного доступа:
- защита базы данных Microsoft Access с помощью пароля и шифрования;
- защита приложения Microsoft Access путем сокрытия объектов в окне базы данных и настройки параметров запуска;
- защита паролем программы на языке VBA;
- защита программ VBA путем создания файла, в котором отсутствует исходный код;
- защита базы данных Microsoft Access и ее объектов средствами защиты на уровне пользователей.

Приложение не всегда нуждается в сложной защите, бывают ситуации, когда вполне достаточно использования пароля. Защита осуществляется таким образом, что только пользователь, точно знающий пароль, может открыть базу данных. Если пользователь забыл пароль, базу данных открыть невозможно. Чтобы снять пароль, его тоже необходимо знать. Однако следует заметить, что установка пароля на базу данных не защищает ее от просмотра различными редакторами или утилитами чтения файлов, поэтому рекомендуется выставлять пароль и шифровать базу данных одновременно. Ввод пароля и шифрование можно применять только к файлам базы данных (например, MDB). Для проектов Access этот метод защиты не применим, так как данные хранятся в таблицах SQL Server и для их защиты используются средства SQL Server. В отличие от баз данных, проект (файл ADP) не может быть защищен с помощью пароля или посредством установки защиты на уровне пользователей средствами Access. Однако, как и в базах данных, в проектах можно защищать паролем программный код на VBA. На практике защита проектов сводится к помещению файла проекта в общую папку на файловом сервере, к которой пользователям сети предоставляется доступ только для чтения. Файл проекта может быть отправлен пользователям по почте. Пользователи должны защитить свою локальную копию файла проекта, используя средства защиты файловой системы личного компьютера, и периодически создавать резервные копии файла проекта при добавлении в него новых форм или отчетов, чтобы в случае повреждения файла проекта иметь возможность его восстановить.

Есть еще способы защиты объектов в базе данных или проекте Access — преобразовать файл в формат MDE или ADE или использовать параметры запуска для ограничения доступа к программам VBA и некоторым параметрам среды Access, можно также скрыть некоторые объекты от пользователей с помощью диалогового окна Параметры (Options). Администрирование баз данных, защищенных с помощью пароля, сводится к изменению пароля защиты (когда это необходимо). Задача администрирования приложений, для которых установлена защита на уровне пользователей, существенно сложнее.

Защита базы данных Access с помощью пароля

Самый простой способ защиты базы данных — с помощью пароля. Можно назначить пароль базе данных Access, который будет требоваться всякий раз при ее открытии.

Установка и снятие пароля защиты базы данных

Чтобы установить пароль для защиты базы данных выполните следующее (пример для интерфейса Access 2003):

1. Закройте базу данных. Если база данных совместно используется в сети, убедитесь, что остальные пользователи ее закрыли.

2. Сделайте резервную копию базы данных и сохраните ее в надежном месте.
3. В меню Access выберите команду Файл, Открыть (File, Open).
4. Выделите файл базы данных.
5. Щелкните по стрелке, расположенной справа от кнопки Открыть (Open) см. рисунок 1. В раскрывающемся списке режимов открытия базы данных выделите элемент Монопольно (Open Exclusive). База данных откроется в режиме монопольного доступа.

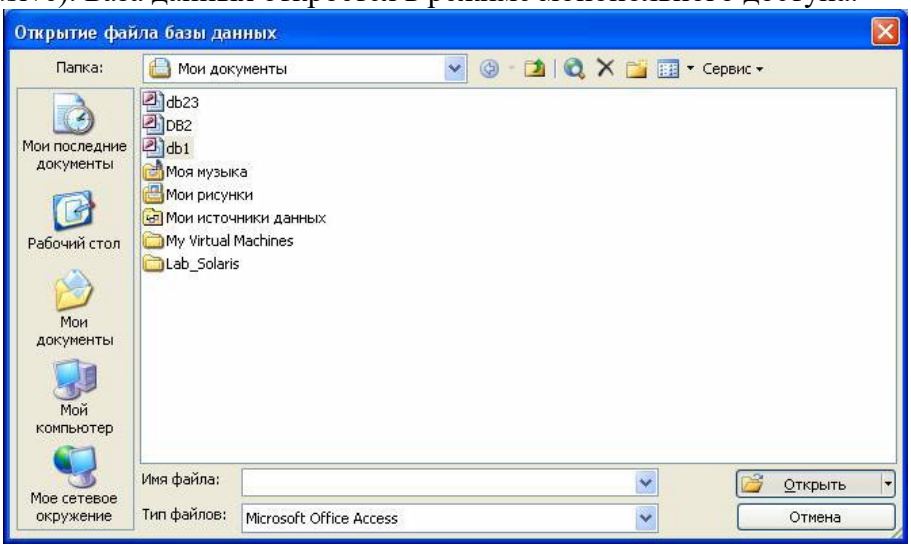


Рисунок 1. Окно открытия базы данных в монопольном режиме.

6. Выберите команду Сервис, Защита, Задать пароль базы данных (Tools, Security, Set Database Password).
7. В появившемся диалоговом окне введите в поле Пароль (Password) пароль для защиты базы данных с учетом регистра символов см. рисунок 2.

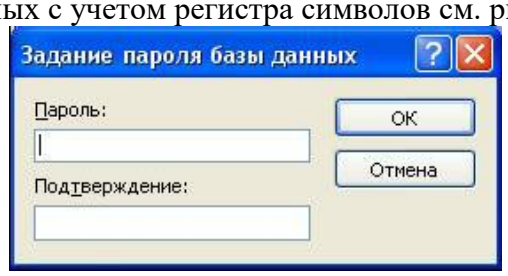


Рисунок 2 - Окно для задания пароля.

8. Введите пароль еще раз в поле Подтверждение (Verify).
9. Нажмите кнопку ОК.

Теперь база данных защищена паролем и всякий раз, когда пользователь будет открывать базу данных, будет отображаться диалоговое окно с требованием ввести пароль. Запомните или сохраните пароль в надежном месте. Если вы забудете пароль, базу данных будет невозможно открыть.

Замечание

Не защищайте базу данных паролем перед ее репликацией (механизм синхронизации содержимого нескольких копий объекта), иначе ее нельзя будет синхронизировать с другими репликами.

Если база данных защищена на уровне пользователей, установить пароль для ее открытия может только пользователь, обладающий административными правами. Установка пароля не влияет на систему защиты на уровне пользователя. Эти два способа защиты могут использоваться одновременно. Пароль базы данных сохраняется в базе данных, а не в файле рабочей группы.

Чтобы удалить пароль защиты базы данных:

1. Откройте базу данных в режиме монопольного доступа.
2. В диалоговое окно необходимо ввести пароль (Password Required) ведите пароль.

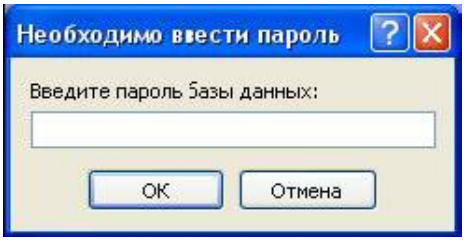


Рисунок 3 - Окно ввода пароля при открытии базы данных.

3. Выберите команду Сервис, Защита, Удалить пароль базы данных (Tools, Security, Unset Database Password). Появится диалоговое окно Удаление пароля базы данных (Unset Database Password) см. рисунок 4.

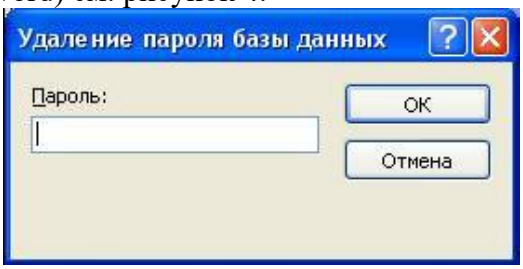


Рисунок 4 - Окно удаления пароля.

4. Введите текущий пароль базы данных.
5. Нажмите кнопку OK.

Установка связи с таблицами базы данных, защищенной паролем

Чтобы установить связь с таблицами базы данных, защищенной паролем, требуется ввести пароль. Если пароль был, указан верно, он сохраняется вместе с другой информацией о ссылках на таблицы. После этого любой пользователь, работающий с базой данных со связанными таблицами, может открыть эти таблицы без указания пароля. Если пароль защищенной базы данных будет изменен, в следующий раз при открытии базы данных, содержащей связанные таблицы, потребуется ввести пароль.

Замечание

Microsoft Access сохраняет пароль в базе данных, содержащей связанные таблицы защищенной базы данных, в незашифрованном виде. Если это уязвляет систему защиты базы данных, не используйте средство защиты с помощью пароля. Установите систему защиты на уровне пользователей, чтобы ограничить доступ к объектам базы данных.

Защита на уровне пользователя

Для этого вида защиты необходимо сначала создать новую рабочую группу (если вы будете использовать старую, то БД легко можно будет вскрыть, т.к. в этом случае для алгоритма защиты будут браться данные, указанные при установке Windows или MS Access).

Для создания новой рабочей группы запустите Сервис, Защита, Администратор рабочих групп и нажмите кнопку Создать (Create…) (рисунок 5).

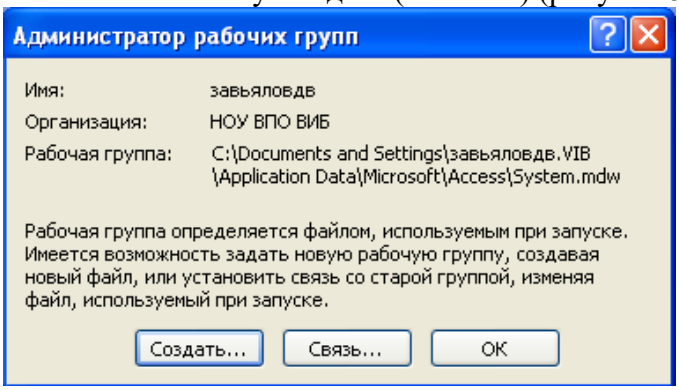


Рисунок 5 - Создание новой рабочей группы

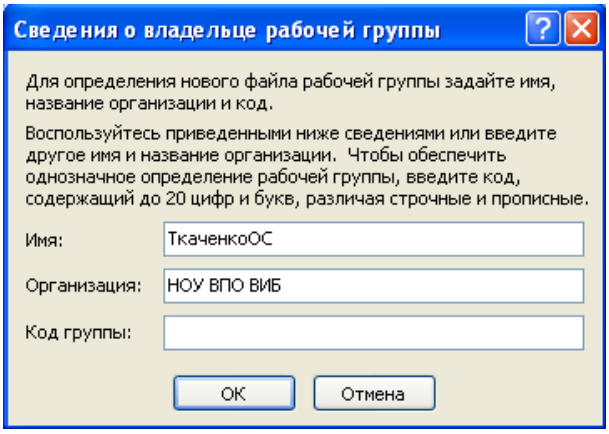


Рисунок 6 - Создание новой рабочей группы

В появившемся диалоге введите запрашиваемую информацию и нажмите кнопку ОК. Задайте имя новой рабочей группы, например MY_GR.MDW.

В случае правильного введения данных и их подтверждения появится сообщение о завершении создания рабочей группы. Теперь можно выйти из программы Администратор рабочих групп.

Запустите БД, которую необходимо защитить. В пункте меню Сервис, Защита, Пользователи и группы (рисунок 7).

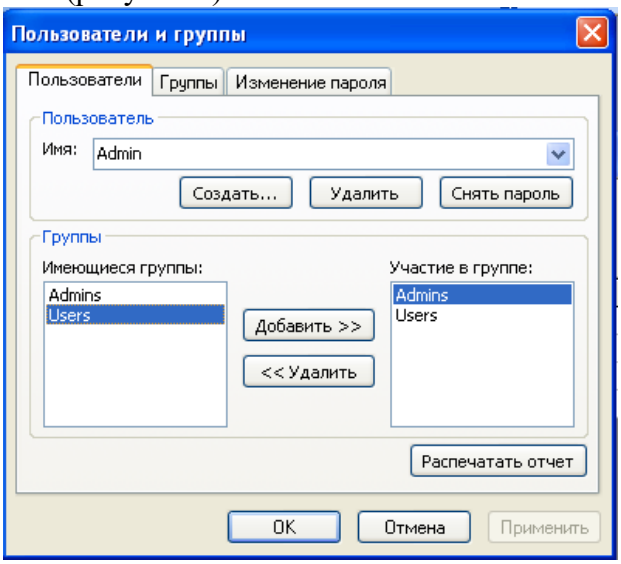


Рисунок 7 - Окно свойств пользователей и групп

Нажмите кнопку Создать… и введите имя нового пользователя, например user1, укажите его код. По умолчанию запись войдет в группу Users. Повторите эти действия для всех пользователей, которые будут работать с БД.

Перейдите в вкладку Изменение пароля. Задайте пароль администратора, после чего при каждом запуске Access будет появляться окно, предлагающее ввести имя пользователя и пароль.

В пункте меню Сервис, Защита, Разрешения (рисунок 8). Выберете защищаемый объект, например Doctors. Задайте разрешения для группы Admin, а затем и для каждого из пользователей.

Остается каждому пользователю самому ввести свой пароль. Для этого необходимо зайти в БД под своим именем и выполнить действия как при создании пароля Администратора.

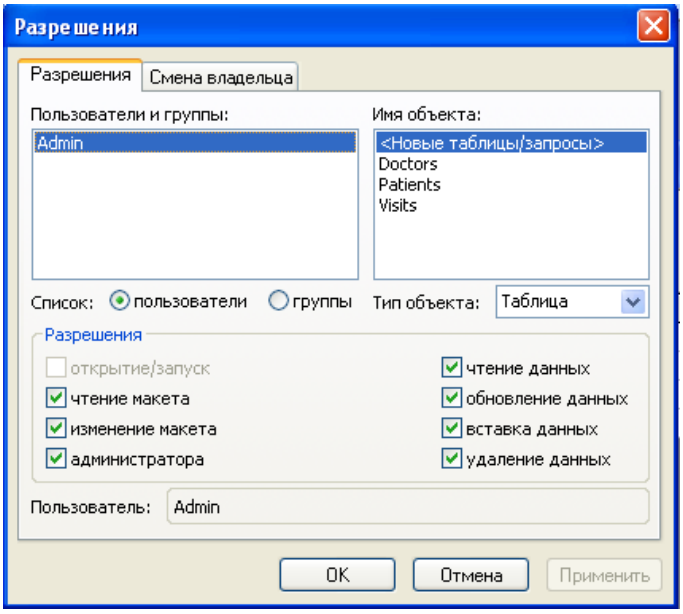


Рисунок 8 - Окно определения прав доступа для каждого пользователя

Шифрование базы данных

При шифровании базы данных ее файл сжимается и делается недоступным для чтения с помощью служебных программ или текстовых редакторов. Дешифрование базы данных отменяет результаты операции шифрования.

Чтобы зашифровать или дешифровать базу данных, нужно сначала ее закрыть, а затем выбрать пункт меню Сервис, Защита, Шифровать/дешифровать (Tools, Sequrity, Encrypt/Decript Database). Затем необходимо указать шифруемый и результирующий файлы в окнах, аналогичных стандартному окну открытия файла.

Задания:

1. Создайте копию базы данных.
2. Закройте паролем свою базу данных. Замените пароль на другой.
3. Создайте свою учетную запись, определите для нее вид доступа и установите пароль.
4. Зашифруйте базу данных и сохраните ее под именем CryptDBI.
5. Расшифруйте базу данных и сохраните ее под именем DBIENCRYPT.

Создание отчета

После выполнение практических заданий студент должен составить электронный отчет по практической работе (в программе Microsoft Word), в котором должны быть отражены следующие положения:

- номер и название практической работы;
- цель и план занятия;
- экранные копии, подтверждающие выполнение практического задания;
- ответы на вопросы:

1) Перечислите способы защиты базы данных Access от несанкционированного доступа.
2) К какому типу файлов можно использовать закрытие паролем и шифрованием.
3) В чем заключается смысл администрирования баз данных, защищенных с помощью пароля.
4) Почему нельзя защищать паролем базу данных перед ее репликацией.
5) Что такое объекты доступа к данным и назовите их модели.

Сохраните отчет на сайте дистанционного обучения для проверки преподавателем.

Тема № 6: «Основные программно-технические меры. Защита информации с помощью пароля»

Практическое задание.
Часть 1. Создание резервных копий файлов (для баз данных и проектов Access)

Цель - изучить способы создания резервных копий базы данных.

Результат обучения. После обучения студент должен:
- знать основные способы создания резервных копий базы данных;
- уметь осуществлять архивирование, сжатие и восстановление баз данных.

Архивирование, сжатие и восстановление баз данных

Чтобы застраховаться от безвозвратной потери данных, в результате целенаправленных действий злоумышленника или по другим причинам необходимо периодически создавать резервную копию базы данных или проекта Access. В случае повреждения файла исходной базы данных или проекта Access его можно будет заменить резервной копией.

Периодичность смены копий зависит скорости обновления данных и определяется администратором базы данных. Чтобы увеличить производительность базы данных и уменьшить ее размер, используйте операцию сжатия базы данных или проекта Access. Начиная с версии Access 2000, сжатие и восстановление базы данных объединены в один процесс.

Создание резервной копии базы данных или проекта Access 2003

Есть несколько путей создания резервной копии базы данных или проекта. При наличии достаточного объема свободного места на диске можно создать резервную копию обычным копированием файла. Создать копию файла можно с помощью приложения Проводник (Explorer), входящего в состав операционной системы Windows, с помощью команды операционной системы copy, с помощью инструкции FileCopy в процедуре на VBA (только, если база данных или проект в это время не открыты в другом окне приложения Access).

Чтобы сэкономить место на диске, создается сжатая копия файла с помощью программы архивирования, например с помощью стандартной утилиты архивирования файлов Backup, входящей в состав операционной системы Windows, или с помощью утилит сторонних производителей, таких как WinZip или WinRar.

Если в базе данных установлена защита на уровне пользователей, необходимо создать также резервную копию соответствующего файла рабочей группы операцией копирования или архивирования соответствующего файла с расширением mdw. Для проектов Access 2003 имеется возможность создания резервной копии средствами Access. С помощью команды Сервис, Служебные программы, Архивировать SQL-базу данных (Tools, Database Utilities, Backup SQL Database) создается резервная копию проекта Access 2003, а затем, при необходимости, восстановить из этой копии сохраненный проект с помощью команды Сервис, Служебные программы, Восстановить SQL-базу данных (Tools, Database Utilities, Restore SQL Database). Можно использовать команду для сохранения данных на SQL Server или MSDE2000 из проекта Access 2003 в виде файла mdf: Сервис, Служебные программы, Копировать файл базы данных (Tools, Database Utilities, Copy Database File).

Еще одна команда Access позволяет удалить источник данных проекта Access 2003 с SQL Server или MSDE2000: Сервис, Служебные программы, Удалить базу данных SQL (Tools, Database Utilities, Drop SQL Database). Раньше для этих целей использовалась утилита Enterprise Manager для SQL Server или специальные инструкции на Transact-SQL. Все эти новые команды работают только, если на компьютере установлен MSDE2000 или SQL Server.

Сжатие базы данных или проекта Access

При удалении данных или объектов файл базы данных или проекта Access становится фрагментированным, это приводит к тому, что дисковое пространство используется неэффективно. Сжатие базы данных или проекта позволяет получить - копию, в которой данные и объекты сохраняются более рационально, что значительно экономит место на диске. Сжатие повышает производительность баз данных и проектов Access. Однако сжатие проекта не влияет на объекты, такие как представления и таблицы, хранящиеся в базе данных на SQL Server. Сжатие проекта не влияет также на таблицы, содержащие поле счетчика в проектах Access, как это происходит с базами данных. Если из базы данных, перед сжатием из таблицы, содержащей поле

счетчика, были удалены последние записи, после сжатия номер первой пустой записи сбрасывается. Добавленная после этого запись получит в поле счетчика номер, на единицу превышающий значение счетчика в последней оставшейся записи.

Перед сжатием совместно используемой базы данных убедитесь, что она не открыта ни одним из пользователей сети. Для сжатия базы данных необходимо обладать правами на ее открытие, запуск и открытие в монопольном режиме. Для сжатия открытой базы данных или проекта Access 2003 необходимо выполнить следующие действия:

1. Перед сжатием сетевой базы данных, расположенной в общей папке или на сервере, убедитесь, что она не открыта другими пользователями.

2. Выберите команду Сервис, Служебные программы, Сжать и восстановить базу данных (Tools, Database Utilities, Compact and Repair Database).

Для сжатия закрытой в данный момент базы данных или проекта Access 2003 необходимо выполнить следующие действия:

1. Если в данный момент открыта другая база данных или проект Access 2003, закройте ее (его). Если база данных или проект расположены в общей папке или на сервере, убедитесь, что они не открыты другими пользователями.

2. Выберите команду Сервис, Служебные программы, Сжать и восстановить базу данных (Tools, Database Utilities, Compact and Repair Database).

3. Появится диалоговое окно База данных для сжатия (Database To Compact From) (рисунок 9), похожее на окно открытия базы данных. Укажите базу данных или проект, который необходимо сжать, и нажмите кнопку Сжать (Compact).

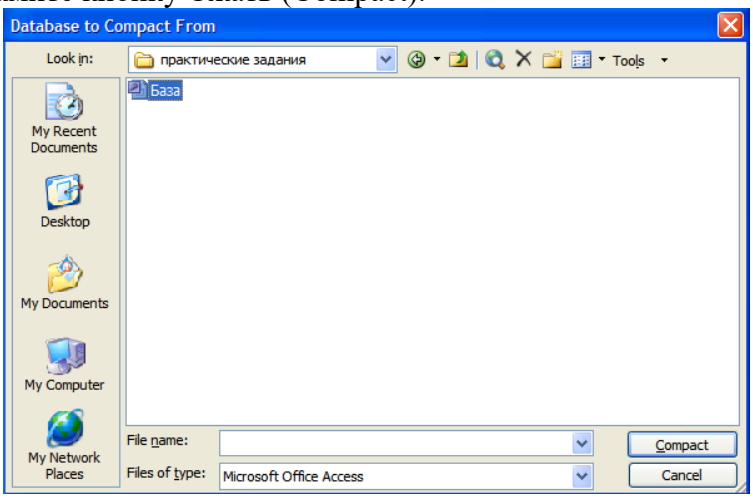


Рисунок 9 - Диалоговое окно База данных для сжатия

4. Появится диалоговое окно Сжатие базы данных под именем (Compact Database Into) (рисунок 10). Выберите диск и папку и введите имя для сохранения сжатой базы данных (необходимо выбрать свою рабочую папку). Нажмите кнопку Сохранить (Save).

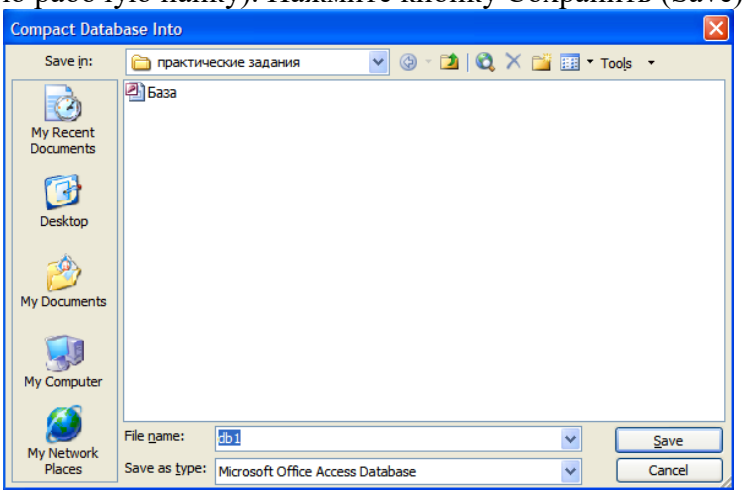


Рисунок 10 - Диалоговое окно Сохранение сжатой базы данных

В обоих случаях процесс сжатия можно прервать с помощью комбинации клавиш <Ctrl>+<Break> или клавиши <Esc>. Допускается сжатие файла базы данных или проекта Access 2003 в файл с тем же именем, что и имя исходного файла, или создание файла с новым именем. При указании того же имени, диска и папки и при успешном сжатии базы данных исходный файл автоматически заменяется на сжатый файл. Можно настроить Access 2003 так, чтобы конкретная база данных илипроект автоматически сжимались при закрытии.

Чтобы установить автоматическое сжатие базы данных Access 2003:

1. Откройте базу данных, которую нужно сжать.

2. Выберите команду Сервис, Параметры (Tools, Options). В появившемся диалоговом окне Параметры (Options) раскройте вкладку Общие (General).

3. Установите флажок Сжимать при закрытии (Compact on Close) и нажмите кнопку ОК.

Установка автоматического сжатия проекта Access 2003 выполняется аналогично.

Автоматическое сжатие не происходит, если при этом размер базы данных (или проекта) не будет уменьшен, по крайней мере, на 256 Кбайт, а также, если эта база данных (или проект) в текущий момент открыта другим пользователем в сети.

Восстановление поврежденной базы данных

В большинстве случаев Microsoft Access определяет, что база данных повреждена, при попытке открыть, зашифровать или дешифровать ее. Тогда пользователю предоставляется возможность восстановить базу данных, выполнив ее сжатие. Но в некоторых ситуациях не удается определить, что база данных повреждена. Если база данных ведет себя непредсказуемым образом, выполните ее сжатие. При серьезных проблемах, которые приводят к вынужденному завершению работы Access, это приложение перезапускается и автоматически создается резервная копия открытой базы данных или проекта Access с тем же именем и расширением, что и исходный файл, только с суффиксом Backup (резервный).

Задания:

1. Оцените эффективность стандартной утилиты архивирования файлов Backup.
2. Выполните сжатие любой базы данных и сохраните под именем CompDBI в своей папке.
3. Настройте Access так, чтобы база данных автоматически сжималась при закрытии.

Часть 2. Защита информации с помощью пароля

Цель - исследование защиты с применением пароля, а также исследование методов противодействия атакам на пароль.

Результат обучения. После обучения студент должен:

- знать основные способы создания резервных копий базы данных;
- уметь осуществлять архивирование, сжатие и восстановление баз данных.

Атаки на пароль

На сегодняшний день пароль является наиболее приемлемым и потому наиболее часто используемым средством установления подлинности, основанным на знаниях субъектов доступа.

В любой критической системе ошибки человека-оператора являются, чуть ли не самыми дорогостоящими и распространенными. В случае криптосистем, непрофессиональные действия пользователя сводят на нет самый стойкий криптоалгоритм и самую корректную его реализацию и применение.

В первую очередь это связано с выбором паролей. Очевидно, что короткие или осмысленные пароли легко запоминаются человеком, но они гораздо проще для вскрытия. Использование длинных и бессмысленных паролей безусловно лучше с точки зрения криптостойкости, но человек обычно не может их запомнить и записывает на бумажке, которая потом либо теряется, либо попадает в руки злоумышленнику. Именно из того, что неискушенные пользователи обычно выбирают либо короткие, либо осмысленные пароли, существуют два метода их вскрытия: атака полным перебором и атака по словарю.

Защищенность пароля при его подборе зависит, в общем случае, от скорости проверки паролей и от размера полного множества возможных паролей, которое, в свою очередь, зависит от длины пароля и размера применяемого алфавита символов. Кроме того, на защищенность сильно влияет реализация парольной защиты.

В связи с резким ростом вычислительных мощностей атаки полным перебором имеют гораздо больше шансов на успех, чем раньше. Кроме того, активно используются распределенные вычисления, т.е. равномерное распределение задачи на большое количество машин, работающих параллельно. Это позволяет многократно сократить время взлома.

Однако вернемся на несколько лет назад, когда вычислительной мощности для полного перебора всех паролей не хватало. Тем не менее, хакерами был придуман остроумный метод, основанный на том, что в качестве пароля человеком выбирается существующее слово или какая-либо информация о себе или своих знакомых (имя, дата рождения и т.п.). Ну, а поскольку в любом языке не более 100000 слов, то их перебор займет весьма небольшое время, и от 40 до 80% существующих паролей может быть угадано с помощью простой схемы, называемой “атакой по словарю”. Кстати, до 80% этих паролей может быть угадано с использованием словаря размером всего 1000 слов!

Пусть сегодня пользователи уже понимают, что выбирать такие пароли нельзя, но, видимо, никогда эксперты по компьютерной безопасности не дождутся использования таких простых и радующих душу паролей, как 34jXs5U@bTa!6;). Поэтому даже искушенный пользователь хитрит и выбирает такие пароли, как hope1, user1997, pAsSwOrD, toor, roottoor, paro1, gfhjkm, asxz. Видно, что все они, как правило, базируются на осмысленном слове и некотором простом правиле его преобразования: прибавить цифру, прибавить год, перевести через букву в другой регистр, записать слово наоборот, прибавить записанное наоборот слово, записать русское слово латинскими буквами, набрать русское слово на клавиатуре с латинской раскладкой, составить пароль из рядом расположенных на клавиатуре клавиш и т.п.

Поэтому не надо удивляться, если такой “хитрый” пароль будет вскрыт хакерами — они не глупее самих пользователей, и уже вставили в свои программы те правила, по которым может идти преобразование слов. В самых "продвинутых" программах (John The Ripper, Password Cracking library) эти правила могут быть программируемыми и задаваться с помощью специального языка самим хакером.

Приведем пример эффективности такой стратегии перебора. Во многих книгах по безопасности предлагается выбирать в качестве надежного пароля два осмысленных слова, разделенных некоторым знаком (например, good!password). Подсчитаем, за сколько времени в среднем будут сломаны такие пароли, если такое правило включено в набор программы-взломщика (пусть словарь 10000 слов, разделительными знаками могут быть 10 цифр и 32 знака препинания и специальных символа, машина класса Pentium со скоростью 15000 паролей/сек):

10000*(32+10)*10000/15000*2=140000 секунд или менее 1.5 дня!

Чем больше длина пароля, тем большую безопасность будет обеспечивать система, так как потребуются большие усилия для его отгадывания. Это обстоятельство можно представить в терминах ожидаемого времени раскрытия пароля или ожидаемого безопасного времени. Ожидаемое безопасное время (Тб) — половина произведения числа возможных паролей и времени, требуемого для того, чтобы попробовать каждый пароль из последовательности запросов. Представим это в виде формулы:

$$T_б = \frac{A^S \bullet t}{2}, \quad (1)$$

где t— время, требуемое на попытку введения пароля, равное E/R; E — число символов в передаваемом сообщении при попытке получить доступ (включая пароль и служебные символы); R — скорость передачи (символы/мин) в линии связи; S — длина пароля; A — число символов в алфавите, из которых составляется пароль. Если после каждой неудачной попытки подбора автоматически предусматривается десятисекундная задержка, то безопасное время резко увеличивается.

Поэтому при использовании аутентификации на основе паролей защищенной системой должны соблюдаться следующие правила:

а) не позволяются пароли меньше 6–8 символов;

б) пароли должны проверяться соответствующими контроллерами;

в) символы пароля при их вводе не должны появляться в явном виде;

г) после ввода правильного пароля выдается информация о последнем входе в систему;

д) ограничивается количество попыток ввода пароля;

е) вводится задержка времени при неправильном пароле;

ж) при передаче по каналам связи пароли должны шифроваться;

з) пароли должны храниться в памяти только в зашифрованном виде в файлах, недоступных пользователям;

и) пользователь должен иметь возможность самому менять пароль;

к) администратор не должен знать пароли пользователей, хотя может их менять;

л) пароли должны периодически меняться;

м) устанавливаются сроки действия паролей, по истечении которых надо связаться с администратором.

Проблема выбора пароля

Выбор длины пароля в значительной степени определяется развитием технических средств, их элементной базы и ее быстродействием. В настоящее время широко применяются многосимвольные пароли, где S>10. В связи с этим возникают вопросы: как и где его хранить и как связать его с аутентификацией личности пользователя? На эти вопросы отвечает комбинированная система паролей, в которой код пароля состоит из двух частей. Первая часть состоит из 3–4-х десятичных знаков, если код цифровой, и более 3–4-х, если код буквенный, которые легко запомнить человеку. Вторая часть содержит количество знаков, определяемое требованиями к защите и возможностями технической реализации системы, она помещается на физическом носителе и определяет ключ-пароль, расчет длины кода которого ведется по указанной выше методике. В этом случае часть пароля будет недоступна для нарушителя.

Однако при расчете длины кода пароля не следует забывать о том, что при увеличении длины пароля нельзя увеличивать периодичность его смены. Коды паролей необходимо менять обязательно, так как за большой период времени увеличивается вероятность их перехвата путем прямого хищения носителя, снятия его копии, принуждения человека. Выбор периодичности необходимо определять из конкретных условий работы системы, но не реже одного раза в год. Причем желательно, чтобы дата замены и периодичность должны носить случайный характер.

Для проверки уязвимости паролей используются специальные контроллеры паролей. Например, известный контроллер Кляйна, осуществляет попытки взлома пароля путем проверки использования в качестве пароля входного имени пользователя, его инициалов и их комбинаций, проверки использования в качестве пароля слов из различных словарей, начиная от наиболее употребительных в качестве пароля, проверки различных перестановок слов, а также проверки слов на языке пользователя–иностранца. Проверка паролей в вычислительных сетях с помощью контроллера Кляйна показала довольно высокие результаты — большинство пользователей используют простые пароли. Показателен пример, когда контроллер Кляйна позволил определить 100 паролей из 5 символов, 350 паролей из 6 символов, 250 паролей из 7 символов и 230 паролей из 8 символов.

Приведенный анализ позволяет сформулировать следующие правила снижения уязвимости паролей и направленные на противодействие известным атакам на них:

- расширяйте применяемый в пароле алфавит — используйте прописные и строчные буквы латинского и русского алфавитов, цифры и знаки;
- не используйте в пароле осмысленные слова;
- не используйте повторяющиеся группы символов;
- не применяйте пароли длиной менее 6–8 символов, так как запомнить их не представляет большого труда, а пароль именно нужно запоминать, а не записывать. По той же причине не имеет смысла требовать длину неосмысленного пароля более 15 символов, так как запомнить его нормальному человеку практически невозможно;

– не используйте один и тот же пароль в различных системах, так как при компрометации одного пароля пострадают все системы;

– проверяйте пароли перед их использованием контроллерами паролей.

Для составления пароля можно дать рекомендации, которыми пользоваться надо очень осторожно:

– выберите несколько строк из песни или поэмы (только не те, которые Вы повторяете первому встречному) и используйте первую (или вторую) букву каждого слова — при этом пароль должен иметь большую длину (более 15 символов), иначе нужно менять регистры букв, применять латинские буквы вместо русских или наоборот, можно вставлять цифры и знаки;

– замените в слове из семи–восьми букв одну согласную и одну или две гласных на знаки или цифры. Это даст вам слово-абракадабру, которое обычно произносимо и поэтому легко запоминается. Подведем итог:

Что такое плохой пароль:

– Собственное имя;
– Слово, которое есть в словаре;
– Идентификатор, присвоенный Вам какой-нибудь системой, или любые его вариации;
– Дата рождения;
– Повторенный символ (например: AAA);
– Пароль меньше 6 символов;
– Пароль, установленный Вам чужим человеком;
– Пароль, состоящий из символов соседствующих на клавиатуре (например: QWERTY или ЙЦУКЕ);
– Пароль состоящий из паспортных данных: персональный номер, номер водительских прав и т.д.

Что такое хороший пароль:

– Бессмысленная фраза;
– Случайный набор символов вперемешку с буквами.

Порядок работы с программами вскрытия паролей.

В данной лабораторной работе используется программный продукт для вскрытия закрытых паролем архивов: Advanced ZIP Password Recovery

Работа с программами взлома на примере AZPR

Программа AZPR используется для восстановления забытых паролей ZIP-архивов. На сегодняшний день существует два способа вскрытия паролей: перебор (brute force) и атака по словарю (dictionary-based attack).

Панель управления:

– кнопки Открыть и Сохранить позволяют работать с проектом, в котором указан вскрываемый файл, набор символов, последний протестированный пароль. Это позволяет приостанавливать и возобновлять вскрытие.

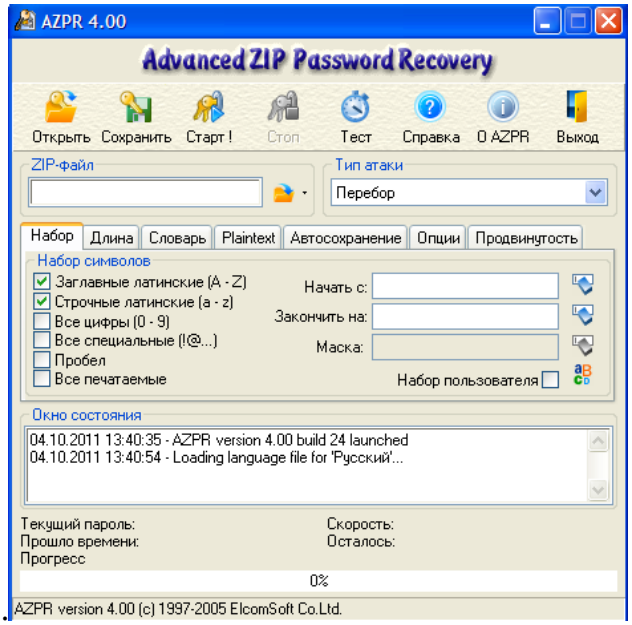
– кнопки Старт и Стоп позволяют соответственно начинать и заканчивать подбор пароля.

– кнопка Набор позволяет задать свое множество символов, если известны символы, из которых состоит пароль.

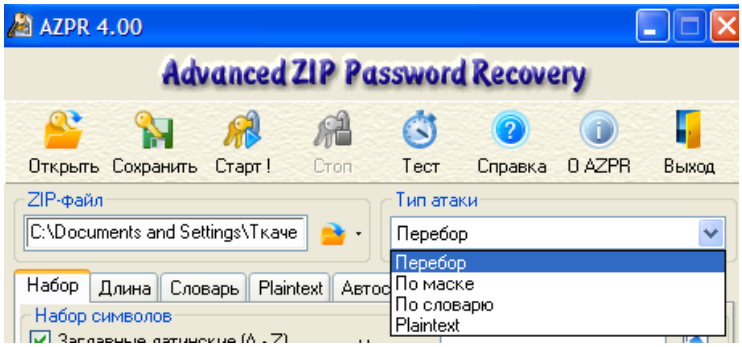
– кнопка Справка выводит помощь по программе.

– кнопка О AZPR выводит информацию о программе.

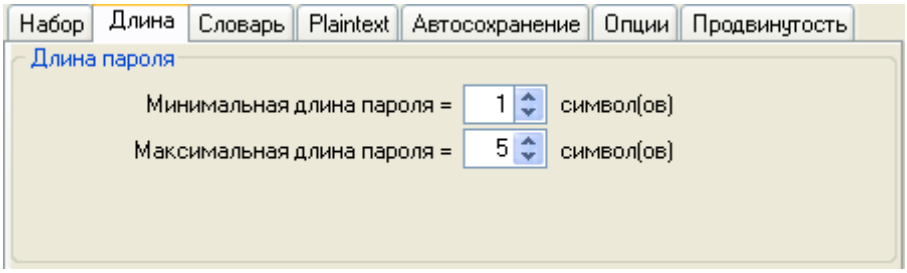
– кнопка Выход позволяет выйти из программы



Рассмотрим возможности программы:
Выбирается архив для вскрытия и тип атаки (см. рисунок).



Выбираются параметры работы:
Закладка Набор
Программа позволяет выбрать область перебора (набор символов). Это значительно сокращает время перебора. Можно использовать набор пользователя, заданный с помощью кнопки Набор. Можно ограничить количество тестируемых паролей, задав начальный пароль. В случае если известна часть пароля, очень эффективна атака по маске. Нужно выбрать соответствующий тип атаки, после этого станет доступным поле маска. В нем нужно ввести известную часть пароля в виде P?s?W?r?, где на месте неизвестных символов нужно поставить знак вопроса. Можно использовать любой другой символ, введя его в поле символ маски.
Закладка Длина



Позволяет выбрать длину пароля.
Закладка Словарь
Позволяет выбрать файл-словарь. Выбирайте файл English.dic, он содержит набор английских слов и наборы символов, наиболее часто использующиеся в качестве паролей.
Закладка Автосохранение

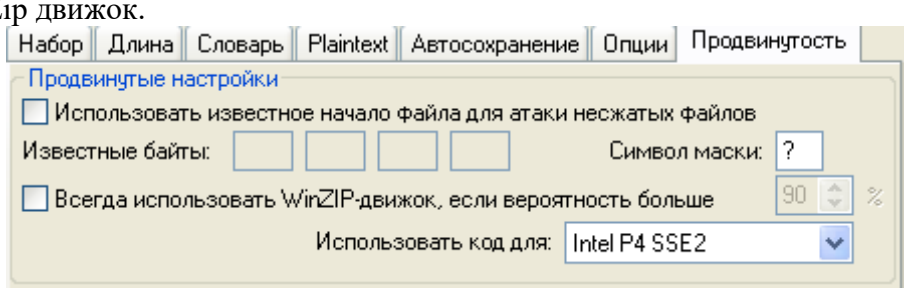
Можно выбрать имя файла для сохранения результатов работы и интервал автосохранения.

Закладка Опции

Выбирается приоритет работы (фоновый или высокий), интервал обновления информации о тестируемом в данный момент пароле. Увеличение интервала повышает быстродействие, но снижает информативность. Также можно установить режим ведения протокола работы и возможность минимизации программы в tray (маленькая иконка рядом с часами).

Закладка Продвинутость

Содержит продвинутые настройки, позволяет использовать известное начало файла, использовать WinZip движок.



Задания:

1. Проведение атаки перебором (bruteforce attack)

Используя программу для вскрытия паролей произвести атаку на зашифрованный файл AZPR.zip. Область перебора – все печатаемые символы, длина пароля от 1 до 5 символов. Время выполнения на компьютере класса Pentium II и выше – 50 секунд – 3 минуты. Проверить правильность определенного пароля, распаковав файл и ознакомившись с его содержимым.

Выполнив пункт 1, сократить область перебора до фактически используемого (например, если пароль grant – то выбрать строчные латинские буквы). Провести повторное вскрытие. Сравнить затраченное время.

2. Проведение атаки по словарю (dictionary attack)

1. Сжать какой-либо небольшой файл, выбрав в качестве пароля английское слово длиной до 5 символов (например, love, god, table, admin и т.д.). Провести атаку по словарю. Для этого выбрать вид атаки и в закладке Словарь выбрать файл English.dic. Он содержит набор английских слов и наборы символов, наиболее часто использующиеся в качестве паролей.

2. Попытаться определить пароль методом прямого перебора. Сравнить затраченное время.

Контрольные вопросы:

1. Для каких целей используются операции сжатие и восстановление базы данных.
2. Перечислите основные способы создания копии базы данных и проектов.
3. Назовите особенности создания копий защищенной базы данных.
4. Перечислите основные способы создания копии и восстановления проекта Access.
5. Какие виды атак на пароль Вы знаете?
6. Что такое плохой пароль?
7. Как можно противостоять атаке полным перебором?
8. Как длина пароля влияет на вероятность раскрытия пароля?
9. Какие рекомендации по составлению паролей Вы можете дать?

Создание отчета

После выполнение практических заданий студент должен составить электронный отчет по практической работе (в программе Microsoft Word), в котором должны быть отражены следующие положения:

- номер и название практической работы;
- цель и план занятия;
- экранные копии, подтверждающие выполнение практического задания;
- ответы на контрольные вопросы:

Сохраните отчет на сайте дистанционного обучения для проверки преподавателем.

Тема № 7: «Защита от несанкционированного доступа и сетевых хакерских атак»

Практическое задание. Защита от несанкционированного доступа и сетевых хакерских атак

Цель - познакомиться с встроенными компонентами защиты операционной системы Microsoft Windows и настроить их

Результат обучения. После обучения студент должен:
- знать общее устройство встроенной защиты Windows;
- уметь настраивать Центр обеспечения безопасности.

Брандмауэр Windows

Задачу защиты от несанкционированного доступа и сетевых атак домашнего компьютера успешно решает персональная программа-брандмауэр. Она может быть как встроенной в операционную систему (например, брандмауэр Windows), так и устанавливаемой отдельно (например Outpost FireWall).

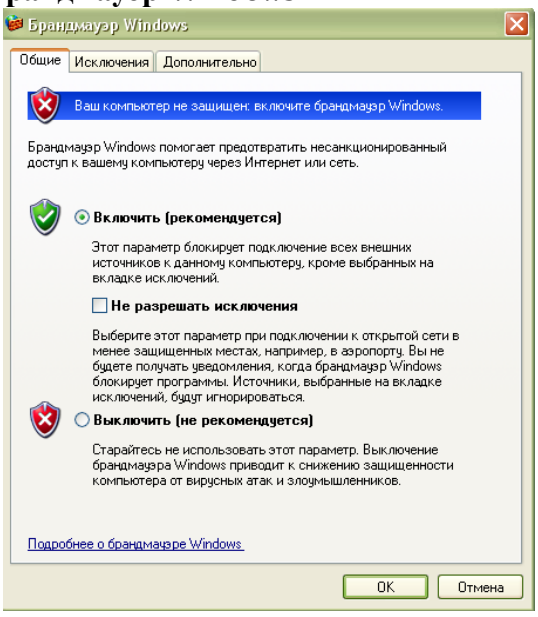
Самая, пожалуй, популярная на сегодняшний день операционная система домашнего компьютера - **Microsoft Windows XP** содержит встроенный **Брандмауэр Windows**. Более поздние версии **Microsoft Windows**, **Vista** и **Seven** содержат в себе дополнительные компоненты защиты от несанкционированного доступа и шпионских программ, например **Windows Defender**.

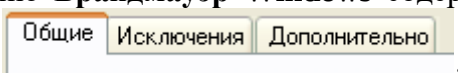
Встроенные брандмауэры отличаются весьма ограниченной функциональностью, что с другой стороны компенсируется отсутствием конфликтов с операционной системой и бесплатностью. Брандмауэры же третьих производителей, устанавливаемые отдельно, обеспечивают обычно более удобную и приятную работу с возможностью более точной настройки различных параметров.

1. После загрузки операционной системы **Microsoft Windows XP** (в Microsoft Virtual PC), **Брандмауэр Windows** будет отключен. Для его включения выполните следующие действия:

Нажмите Меню Пуск – Панель управления – Брандмауэр Windows

На экране появится меню **Брандмауэр Windows**



2. Меню **Брандмауэр Windows** содержит 3 вкладки – **Общие, Исключения, Дополнительно** 

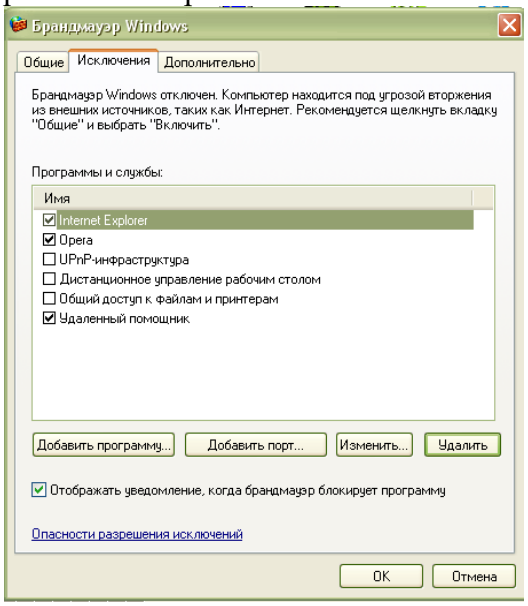
.

Выберите каждую вкладку и просмотрите ее содержимое.

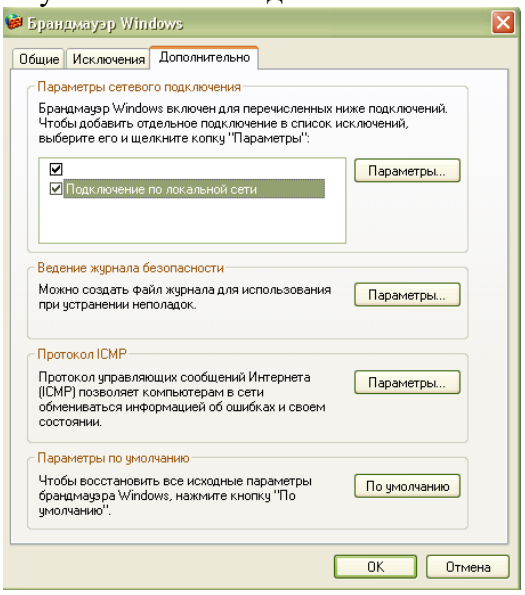
3. Вкладка **Общие** позволяет менять режим работы **Брандмауэра Windows**. Можно **Включить брандмауэр** (после установки Операционной системы **Microsoft**

Windows XP, система автоматически включает **Брандмауэр Windows**) или **Выключить** его (при установке другого Брандмауэра на ваш компьютер, Брандмауэр Windows будет выключен автоматически). Отключите **Брандмауэр Windows**, а затем вновь включите его.

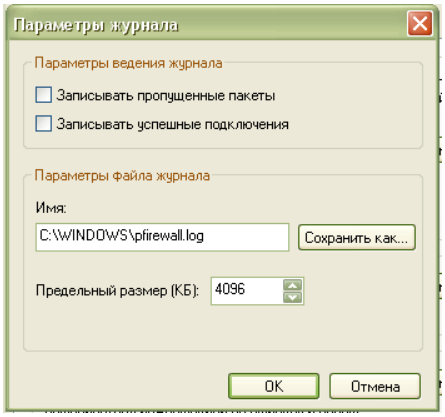
4. Вкладка **Исключения** позволяет создавать исключения для нужных служб и приложений. Например, если вы точно уверены, что конкретное приложение не будет выполнять несанкционированных удаленных соединений или **Брандмауэр Windows** заблокировал сетевой доступ приложения, можно создать Исключение и блокировка будет снята. Добавьте исключение для программы, нажав кнопку **Добавить программу** и в появившемся списке выберите любое приложение.



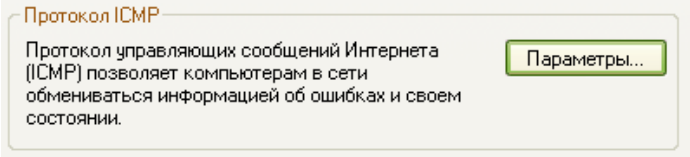
5. Вкладка **Дополнительно** позволяет включить или отключить **Брандмауэр Windows** для конкретных сетевых подключений, заблокировать или разблокировать сетевые службы. Выберите нужно сетевое Подключение и нажмите кнопку **Параметры**



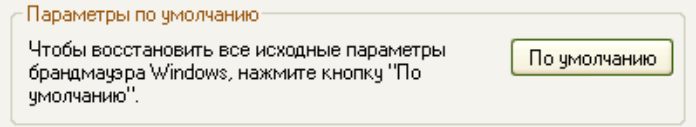
6. При устранении неполадок, можно воспользоваться **Журналом Безопасности**, для того, чтобы выяснить, когда произошла неполадка и при каких обстоятельствах. Нажмите кнопку **Параметры** в блоке **Ведение журнала** безопасности. В появившемся окне произведите настройки, согласно предложенному рисунку и нажмите **Ок**.



7. Блок **Протокол ICMP** служит для приема и отправки сообщений об ошибках и состоянии компьютеров в сети. Так же этот протокол используют некоторые вредоносные программы, с периодичностью показывая различные сообщения о якобы произошедших ошибках в операционной системе.



8. Блок **Параметры по умолчанию** служит для восстановления исходных настроек **Брандмауэра Windows**.



Центр Обеспечения безопасности Windows

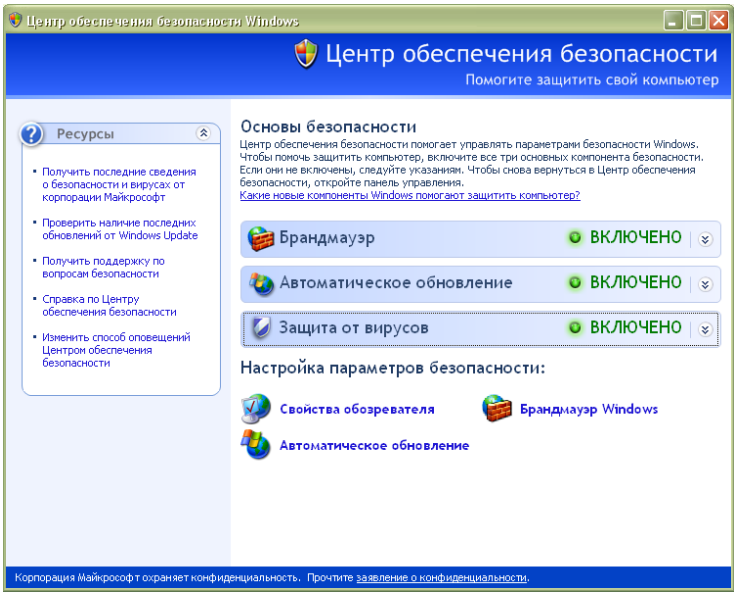
Если ваш компьютер подключен к компьютерной сети (неважно, Интернет это или Интранет), то он уязвим для вирусов, атак злоумышленников и других вторжений. Для защиты компьютера от этих опасностей необходимо, чтобы на нем постоянно работали межсетевой экран (брандмауэр) и антивирусное ПО (с последними обновлениями). Кроме того, необходимо, чтобы все последние обновления были также установлены на вашем компьютере.

Не каждый пользователь может постоянно следить за этим. Не каждый пользователь знает, как это осуществить. И даже если пользователь компетентен в этих вопросах, у него просто может не хватать времени на такие проверки. Компания Microsoft позаботилась обо всех этих пользователях, включив в состав SP2 (и SP3) для Windows XP такой инструмент. Он называется **Центр обеспечения безопасности Windows** (**Windows Security Center**).

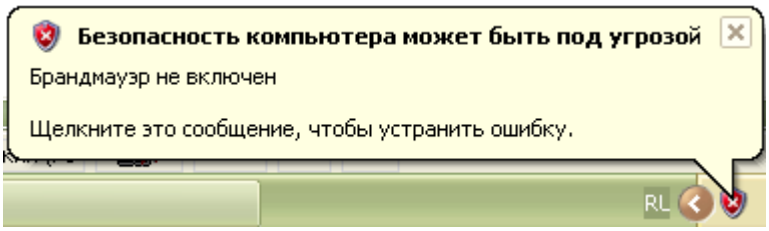
1. Нажмите Меню Пуск – Панель управления – Центр обеспечения безопасности

Для включения Центра обеспечения безопасности Windows, нажмите Пуск – Панель управления – Администрирование – Службы. В списке служб найдите службу Security Center, нажмите 2 раза на на этой службе, выберите тип запуска Авто, нажмите кнопку Применить и ОК. Перезагрузите виртуальную машину.

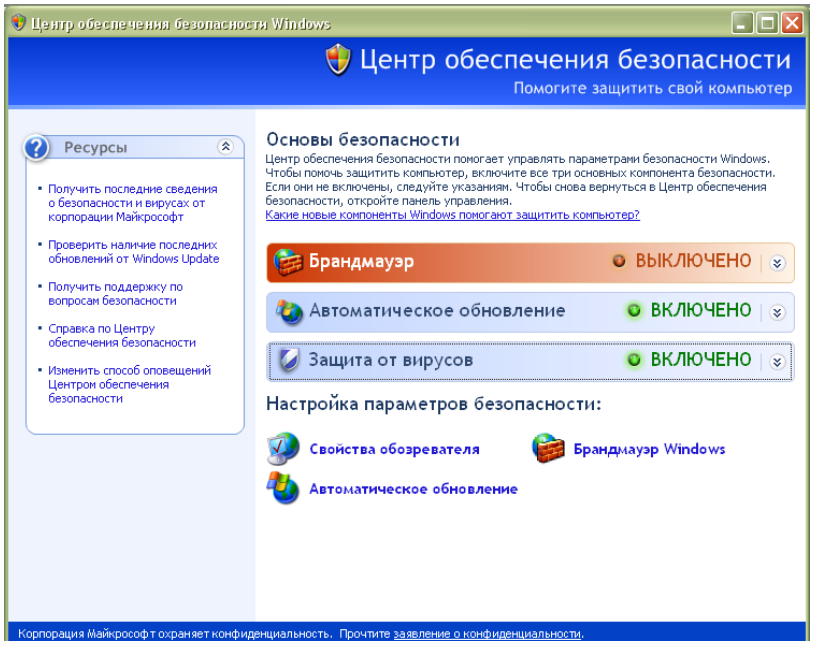
2. На экране появится меню **Центра обеспечения безопасности Windows**.



3. Основное назначение этого инструмента - информировать и направлять пользователя в нужном направлении. Во-первых, он постоянно контролирует состояния трех основных компонентов ОС (брандмауэр, антивирус, система автоматического обновления). Если параметры любого из этих компонентов не будут удовлетворять требованиям безопасности компьютера, то пользователь получит соответствующее уведомление.



4. Меню **Центра обеспечения безопасности Windows** можно разделить на 3 части:

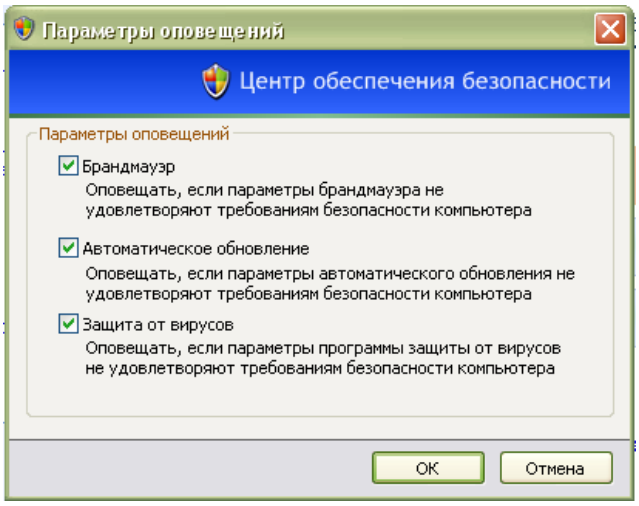


- Ресурсы. Здесь располагаются ссылки для перехода к Интернет-ресурсам, к встроенной в Windows справочной службе и к окну настройки параметров оповещений.

- Компоненты безопасности. Здесь располагаются информационные элементы трех основных компонентов безопасности: брандмауэр, автоматическое обновление, антивирусная защита.
- Параметры безопасности. Здесь располагаются кнопки перехода к настройкам безопасности следующих компонентов: Свойства обозревателя, Автоматическое обновление, Брандмауэр Windows.

Рассмотрим эти части более подробно.

5. В части 1 первые три ссылки предназначены для перехода на соответствующие страницы на сайте Microsoft. Предпоследняя ссылка предназначена для открытия справочной службы Windows на странице "Общие сведения о центре обеспечения безопасности Windows". Последняя ссылка предназначена для открытия окна "Параметры оповещений".



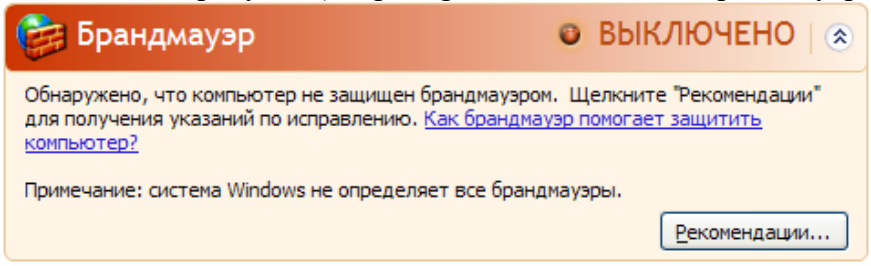
Если на компьютере установлен брандмауэр и антивирусное ПО, не определяемое Центром обеспечения безопасности, вы можете отключить соответствующие оповещения

6. В части 2 каждое информационное табло сообщает о состоянии соответствующего компонента. На рисунке представлены возможные состояния.

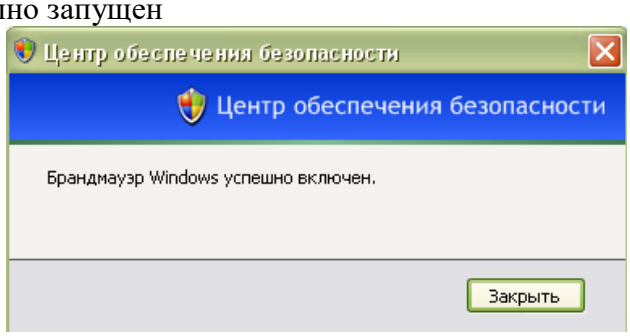
A	ВКЛЮЧЕНО
B	ПРОВЕРЬТЕ ПАРАМЕТРЫ
C	ВЫКЛЮЧЕНО
D	НЕ НАЙДЕНО
E	СРОК ИСТЕК
F	НЕ НАБЛЮДАЕТСЯ

Состояния A-C понятны без комментариев. Состояние D - "Не найдено" - соответствует невозможности определить присутствие соответствующего ПО (например, антивирус или брандмауэр). Состояние E - "Срок истек" - возможно для антивирусной защиты, когда обновления антивирусных баз устарели. Состояние F - "Не наблюдается" - соответствует отключенному контролю над соответствующим компонентом.

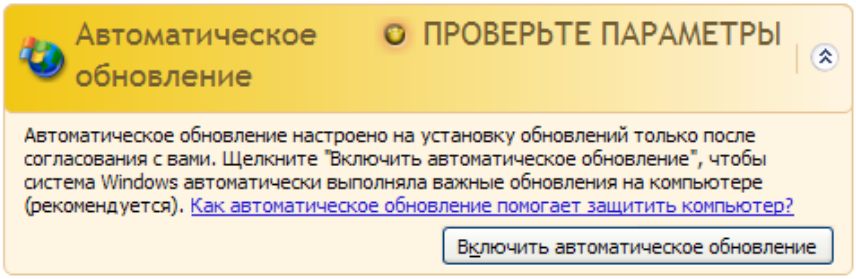
7. Выключите один из компонентов защиты. Состояние этого компоненты примет вид, показанный на рисунке (например, если отключить Брандмауэр Windows)



8. Включите отключенный компоненты защиты, на экране появится сообщение Ваш компонент успешно запущен

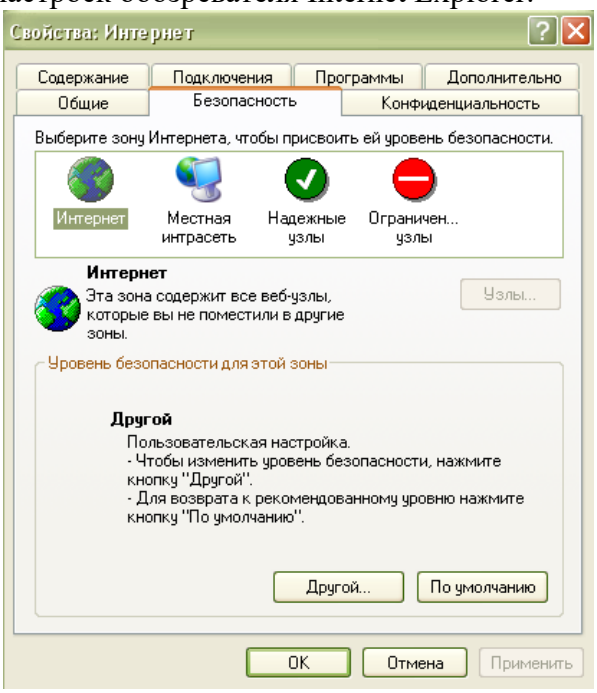


9. Если один из компонентов не может выполнить нужное действие (например, автоматические обновления устанавливаются по выбору пользователя), статус компонента примет вид, показанный на рисунке.

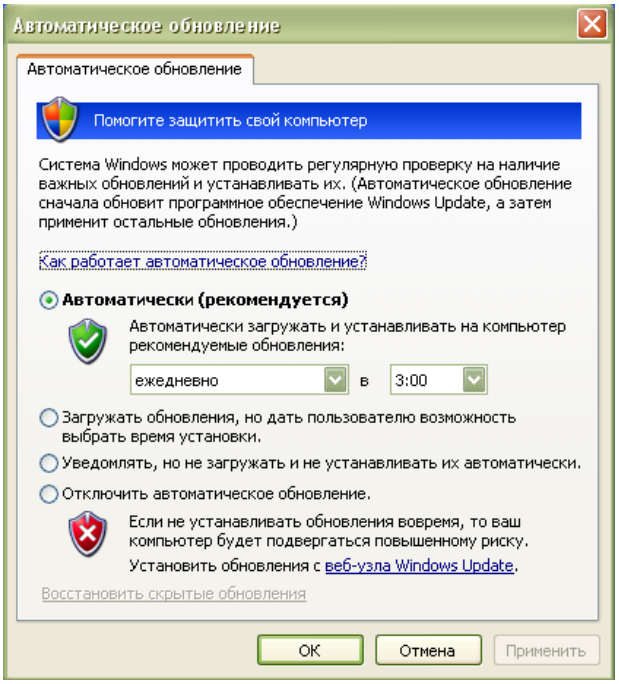


10. Как уже было указано ранее, в разделе 3 расположены кнопки перехода к настройкам безопасности следующих компонентов: обозреватель Internet Explorer, автоматическое обновление, брандмауэр Windows.

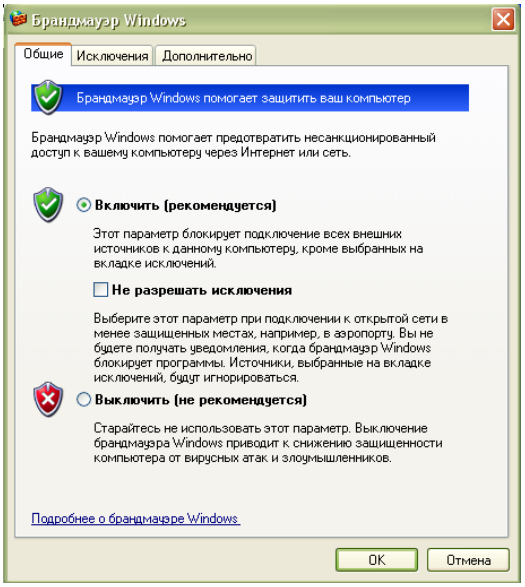
11. Нажав кнопку Свойства обозревателя, вы попадете на закладку "Безопасность" в окне настроек обозревателя Internet Explorer.



12. Нажав кнопку Автоматическое обновление, вы откроете окно настроек "Автоматического обновления".



13. Нажав кнопку Брандмауэр Windows, вы попадете в соответствующее окно настроек.



Задания:

1. Включить Брандмауэр Windows и добавить на вкладке Исключения несколько программ или служб исключений.
2. Настройте Брандмауэр так, чтобы в журнале безопасности записывались пропущенные пакеты.
3. Какие настройки Брандмауэра необходимо использовать, чтоб восстановить значения по умолчанию? Продемонстрируйте.

Контрольные вопросы:

Создание отчета

После выполнение практических заданий студент должен составить электронный отчет по практической работе (в программе Microsoft Word), в котором должны быть отражены следующие положения:

- номер и название практической работы;
- цель и план занятия;
- экранные копии, подтверждающие выполнение практического задания;

- ответы на вопросы:
  1. Для чего используется Брандмауэр Windows?
  2. Какие действия необходимо выполнить для активации Брандмауэра Windows?
  3. Как создать исключение в Брандмауэре Windows?
  4. Для чего используется Центр обеспечения безопасности Windows?
  5. Как центр обеспечения безопасности уведомляет пользователя об отключенном компоненте защиты?
  6. Какие компоненты защиты настраиваются в Центре обеспечения безопасности?
- Сохраните отчет на сайте дистанционного обучения для проверки преподавателем.

Тема № 8: «Современные антивирусные программы. Защита от информационных инфекций. Классификация компьютерных вирусов»

Практическое занятие. Настройка антивирусной системы безопасности

Цель - изучить общие принципы работы антивирусного программного обеспечения.

Результат обучения. После обучения студент должен:
- знать общие принципы работы антивирусного программного обеспечения;
- уметь настраивть антивирусную систему безопасности.

Установка бесплатную версию «Антивируса Касперского».

После принятия лицензионного соглашения предлагается выбрать один из двух вариантов установки:

• Быстрая установка – будут установлены все компоненты программы с параметрами работы по умолчанию;

• Выборочная установка – установка отдельных компонентов с возможностью предварительной настройки; данный режим рекомендуется для опытных пользователей. Рекомендуется выбрать быструю установку: в этом случае будет обеспечена максимальная защита компьютера.

Если в каком-либо модуле не будет необходимости, его всегда можно отключить. Далее мастер проверит установленные программы и, если найдет несовместимые с антивирусом, выведет их список. Если вы продолжите установку, данные приложения будут удалены во избежание конфликтов. Если будут найдены конфигурационные файлы от предыдущей установки «Антивируса Касперского», последует запрос на сохранение этих параметров. Если программы, мешающие работе антивирусу, удалялись, после этого, возможно, потребуется перезагрузка компьютера.

В «Антивирусе Касперского», после установки программы запустится Мастер предварительной настройки. Если был выбран вариант Быстрая установка, мастер предложит активизировать продукт.

Выполните установку и настройку антивирусной программы.

Скопируйте в отчет экранные копии установки и настройки программы.

Самостоятельно установите еще одну антивирусную программу (на ваш выбор).

Создание отчета

После выполнение практических заданий студент должен составить электронный отчет по практической работе (в программе Microsoft Word), в котором должны быть отражены следующие положения:
- номер и название практической работы;
- цель и план занятия;
- экранные копии, подтверждающие выполнение практического задания;
- Сохраните отчет на сайте дистанционного обучения для проверки преподавателем.

Тема № 9. Основы технологии построения защищенных ОС

Практическая работа. Основные признаки присутствия на компьютере вредоносных программ

Цель - получение практических навыков по выявлению вредоносных программ на локальном компьютере под управлением Microsoft Windows XP

Результат обучения. После обучения студент должен:
- знать основные настройки свойств обозревателя;
- знать общие принципы работы с диспетчером задач.

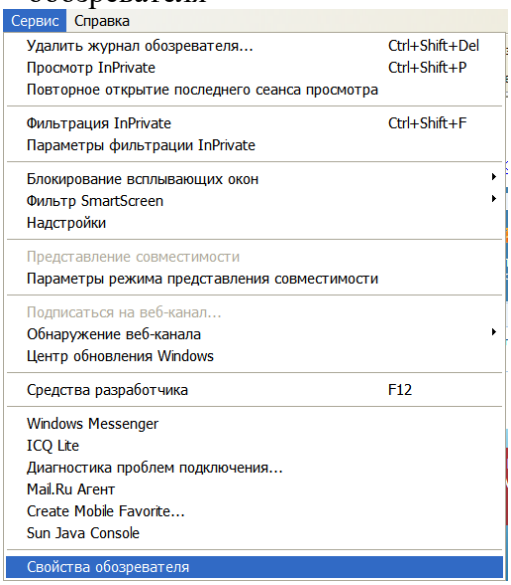
Задание 1. Изучение настроек браузера

Вирусные проявления бывают явными, косвенными и скрытыми. Если первые обычно видны невооруженным глазом, то косвенные и тем более скрытые требуют от пользователя проявления изрядной доли интуиции. Они часто не мешают работе, и для их обнаружения требуется знать, где и что нужно искать.

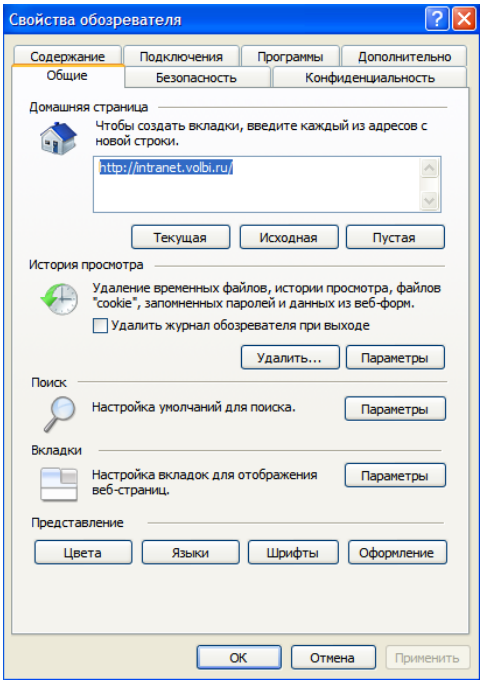
Явные проявления обычно выражаются в неожиданно появляющихся рекламных сообщениях и баннерах - обычно это следствие проникновения на компьютер рекламной утилиты. Поскольку их главная цель - это привлечь внимание пользователя к рекламируемой услуге или товару, то им сложно оставаться незаметными. Также, явные проявления могут вызывать ряд троянских программ, например утилиты несанкционированного дозвона к платным сервисам.

В этом задании предлагается исследовать явные проявления вирусной активности на примере несанкционированного изменения настроек браузера.

1. Откройте браузер Internet Explorer, воспользовавшись одноименным ярлыком на рабочем столе или в системном меню Пуск, Программы 
2. Проверьте значение параметра, отвечающего за стартовую страницу. Для этого нужно воспользоваться меню Сервис. Откройте его и выберите пункт Свойства обозревателя



3. Адрес стартовой страницы указан в первом же поле открывшегося окна Свойства обозревателя, на закладке Общие. Значение этого поля совпадает с тем адресом, который был автоматически задан при открытии браузера. Установите свою стартовую страницу.



4. Далее для подтверждения сделанных изменений нажмите ОК
5. Закройте и снова откройте браузер
6. Убедитесь, что теперь первым делом была загружена страница ваша домашняя страница

Таким образом, если Ваш браузер начал самостоятельно загружать посторонний сайт, в первую очередь нужно изучить настройки браузера: какой адрес выставлен в поле домашней страницы.

Ряд вредоносных программ ограничиваются изменением этого параметра и для устранения последствий заражения нужно лишь исправить адрес домашней страницы. Однако это может быть только частью вредоносной нагрузки. Поэтому если Вы обнаружили несанкционированное изменение адреса домашней страницы, следует немедленно установить антивирусное программное обеспечение и проверить весь жесткий диск на наличие вирусов.

Задание 2. Подозрительные процессы

Одним из основных проявлений вредоносных программ является наличие в списке запущенных процессов подозрительных программ. Исследуя этот список, и особенно сравнивая его с перечнем процессов, которые были запущены на компьютере сразу после установки системы, то есть до начала работы, можно сделать достаточно достоверные выводы об инфицировании. Это часто помогает при обнаружении вредоносных программ, имеющих лишь только скрытые или косвенные проявления.

Однако необходимо четко понимать и уметь отличать легальные процессы (например, системные или запущенные программы) от подозрительных. В этом задании необходимо ознакомиться с основным методом исследования запущенных процессов, а именно получить навыки работы с Диспетчером задач Windows, и изучить стандартный их набор.

Диспетчер задач Windows — это стандартная утилита, входящая в любую версию Microsoft Windows. С ее помощью можно в режиме реального времени отслеживать выполняющиеся приложения и запущенные процессы, оценивать загруженность системных ресурсов компьютера и использование сети.

1. Запустите компьютер.
2. Выключите все программы, которые автоматически запустились при старте ПК.
3. Перейдите к Диспетчеру задач Windows, нажав одновременно клавиши Ctrl+Alt+Delete.

Открывшееся окно содержит закладки, отвечающие разным видам активности, которые отслеживает Диспетчер: приложения, процессы, быстродействие (использование системных ресурсов) и Сеть.

4. Перейдите на вкладку Процессы и внимательно изучите представленный в окне список процессов. Если на компьютере не запущены никакие пользовательские программы, он должен содержать только служебные процессы операционной системы.

5. Для каждого процесса выводятся его параметры: имя образа (может не совпадать с именем запускаемого файла), имя пользователя, от чьего имени был запущен процесс, загрузка этим процессом процессора и объем занимаемой им оперативной памяти.

6. Поскольку в после загрузки не должна быть запущена ни одна пользовательская программа, процессор должен быть свободен. Следовательно, «Бездействие системы» должно оказаться внизу списка с достаточно большим процентом «использования» процессора. Порядка 99 %.

В ряде случаев может потребоваться вручную завершить некий процесс. Это можно сделать с помощью кнопки Завершить процесс.

Например, Вы обнаружили подозрительный процесс, прочитали в сети, что он однозначно принадлежит вирусу или троянской программе, но антивирусной программы на компьютере нет. Тогда нужно закрыть все работающие приложения и с помощью Диспетчера задач вручную завершить этот процесс. Чтобы исключить появление его снова необходимо установить полноценное антивирусное приложение и сразу же запустить проверку всего жесткого диска на наличие вирусов.

7. Не закрывая окна Диспетчера задач Windows, откройте программу Paint. Для этого воспользуйтесь системным меню Пуск, Программы, Стандартные, Paint

8. Дождитесь запуска Paint

9. Не закрывая приложение Paint, вернитесь к окну Диспетчера задач Windows и проследите за изменениями на закладке Приложения

10. Список запущенных приложений должен содержать строку, соответствующею Paint. Поскольку она сейчас работает, это же записано в строке Состояние.

Иногда случается так, что программа вызывает ошибку - тогда в ее состоянии будет написано «Не отвечает». Если некое ранее бесперебойно работающее приложение начало часто без видимых причин переходить в состояние «Не отвечает», это может быть косвенным признаком заражения.

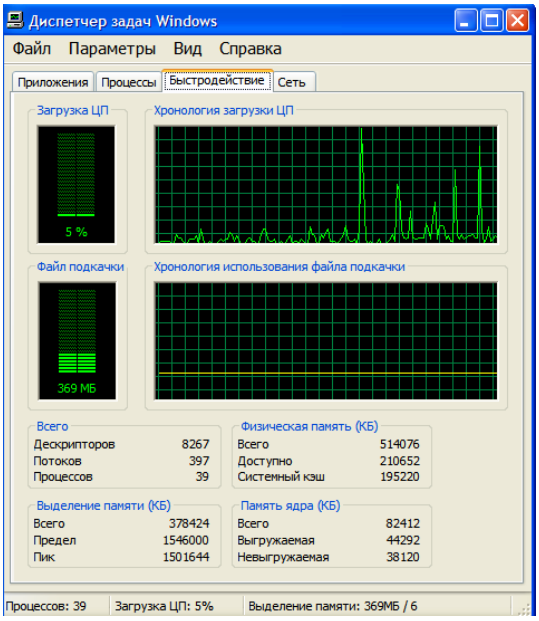
Тогда первое, что можно сделать — это воспользоваться кнопкой Снять задачу и начать поиски причин. Если программа по-прежнему не завершила работу, перейдите на вкладку Процессы, найдите в списке процессов нужный Вам процесс и воспользуйтесь кнопкой Завершить процесс.

11. Убедитесь, что программе Paint соответствует процесс mspaint.exe. Для этого найдите его в списке запущенных процессов, не закрывая и не сворачивая окно Диспетчера задач Windows, вернитесь в окне Paint и закройте его

12. Проследите, что из списка запущенных процессов пропал mspaint.exe

13. Перейдите к закладке Быстродействие

14. Внимательно изучите расположенные тут графики. Любые всплески на них должны по времени соответствовать неким действиям, например запуску требовательной к ресурсам программы. Если ничего похожего сознательно не производилось, это может быть причиной для более детального исследования компьютера



15. Закройте окно Диспетчера задач Windows

Задание 3. Элементы автозапуска

Для того чтобы прикладная программа начала выполняться, ее нужно запустить. Следовательно, и вирус нуждается в том, чтобы его запустили. Для этого можно использовать два сценария: либо сделать так, чтобы пользователь сам его запустил (либо по незнанию, либо с использованием обманных методов), либо внедриться в конфигурационные файлы и запускать одновременно с другой, полезной программой. Оптимальным с точки зрения вируса вариантом служит запуск одновременно с операционной системой - в этом случае запуск практически гарантирован.

1. Самый простой способ добавить какую-либо программу в автозагрузку — это поместить ее ярлык в раздел Автозагрузка. По умолчанию, сразу после установки операционной системы этот раздел пуст, поскольку ни одной прикладной программы еще не установлено.
2. Проверьте папку Автозагрузка на Вашем компьютере. Она должна быть пустой, если вы не установили программы для запуска.
3. Добавьте в список автозагрузки любую программу (создайте ярлык на любую программу, например Калькулятор или Блокнот и поместите его в группу Автозагрузка).
4. Перезагрузите компьютер.
5. Убедитесь, что по завершению загрузки автоматически запустилась только добавленная программа.
6. Если запустились и другие программы, то это может быть по причине наличия вирусов.

Создание отчета

После выполнение практических заданий студент должен составить электронный отчет по практической работе (в программе Microsoft Word), в котором должны быть отражены следующие положения:

- номер и название практической работы;
- цель и план занятия;
- экранные копии, подтверждающие выполнение практического задания.

Письменно ответьте на контрольные вопросы:

1. Какие настройки браузера могут быть несанкционированно изменены вирусной программой?
2. Какие действия необходимо провести при обнаружении подозрительных процессов с помощью Диспетчера задач?
3. Укажите основные системные процессы, которые необходимы для бесперебойной работы ОС

Сохраните отчет на сайте дистанционного обучения для проверки преподавателем.

5.3. Тематика письменных работ обучающихся

В течение изучения дисциплины «Информационная безопасность» обучающиеся должны сдать и отчитать реферат по одной из предложенных ниже тем:

1. Концепция национальной безопасности.
2. Основные виды угроз информационной безопасности.
3. Законодательный уровень информационной безопасности: обзор российского законодательства.
4. Законодательный уровень информационной безопасности: обзор зарубежного законодательства.
5. Обзор действующих стандартов и рекомендаций в области информационной безопасности.
6. Административный уровень информационной безопасности.
7. Модели основных политик безопасности.
8. Процедурный уровень информационной безопасности.
9. Идентификация, аутентификация с помощью биометрических параметров.
10. История криптографии.
11. Основные понятия и определения криптологии.
12. Симметричные методы шифрования.
13. Ассиметричные методы шифрования.
14. Цифровая подпись: основные понятия.
15. История возникновения электронной цифровой подписи.
16. Алгоритмы ЭЦП.
17. Защита информации от утечки по техническим каналам.
18. Способы несанкционированного доступа к информации.
19. Технические средства несанкционированного доступа.
20. Системы защиты от несанкционированного доступа.
21. Защита от информационных инфекций.
22. Вирус: основные понятия, виды.
23. Троянский конь как одна из угроз безопасности информации.
24. Сетевые черви: милые создания или угроза информационной безопасности.
25. Профилактика и лечение информационных инфекций.
26. Программы обнаружения и защиты от вирусов.
27. Современные антивирусные программы (на примере трех программ).
28. Методы обнаружения и удаления вирусов.
29. Общая характеристика организационных методов защиты.
30. Организационные каналы передачи информации.

5.4. Перечень вопросов промежуточной аттестации по дисциплине

Вопросы к экзамену:

1. Информационная безопасность, как часть эксплуатации современных информационных систем.
2. Организация ИТ-инфраструктуры и управление информационной безопасностью. Доступность, целостность и конфиденциальность информации.
3. Доктрина информационной безопасности РФ.
4. Обзор действующих стандартов и рекомендаций в области информационной безопасности.
5. Классификация защищаемой информации по степени важности и ценности.
6. Основные определения и критерии классификации угроз.
7. Законодательный уровень информационной безопасности.
8. Административный уровень информационной безопасности.
9. Управление информационной безопасностью. Политика безопасности. Содержание политики безопасности. Программа безопасности.
10. Модели основных политик безопасности.

11. Управление рисками. Основные понятия. Подготовительный этап управления рисками.
12. Управление рисками. Основные этапы управления рисками.
13. Методы и модели анализа угроз.
14. Поддержание работоспособности. Реагирование на нарушения режима безопасности.
15. Основные программно-технические меры.
16. Архитектурная безопасность.
17. Идентификация и аутентификация, управление доступом.
18. Идентификация, аутентификация с помощью биометрических параметров.
19. Мониторинг и аудит.
20. История криптографии. Основные понятия и определения криптологии.
21. Шифрование, контроль целостности.
22. Симметричные методы шифрования. Ассиметричные методы шифрования.
23. Цифровая подпись: основные понятия. Алгоритмы ЭЦП.
24. Экранирование, анализ защищенности.
25. Классификация межсетевых экранов.
26. Обеспечение высокой доступности.
27. Вирус: основные понятия, виды. Современные антивирусные программы (на примере трех программ).
28. Методы обнаружения и удаления вирусов.

Раздел 6. Перечень учебной литературы, необходимой для освоения дисциплины

6.1. Основная литература

1. Никифоров, С. Н. Защита информации. Защита от внешних вторжений : учебное пособие / С. Н. Никифоров. — Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 84 с. — ISBN 978-5-9227-0757-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/74381.html
2. Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 424 с. — ISBN 978-5-4497-0336-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/89451.html
3. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/87995.html

6.2. Дополнительная литература

4. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности : учебное пособие / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 431 с. — ISBN 978-5-4497-0935-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102070.html
5. Рагозин, Ю. Н. Инженерно-техническая защита информации : учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности / Ю. Н. Рагозин ; под редакцией Т. С. Кулакова. — Санкт-Петербург : Интермедия, 2018. — 168 с. — ISBN 978-5-4383-0161-5. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/73641.html.
6. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю. Н. Сычев. — Саратов : Вузовское образование, 2018. — 195 с. — ISBN 978-5-4487-0128-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/72345.html

6.3. Другие источники информации и средства обеспечения освоения дисциплины

7. Журнал «Бизнес. Образование. Право. Вестник Волгоградского института бизнеса» // URL: http://vestnik.volbi.ru/
8. Журнал «Мир ПК» // URL: http://www.osp.pcworld
9. Журнал «Компьютерра-онлайн» // URL: http://www2.computerra.ru
10. Журнал «Хакер» // URL: http://www.xakep.ru
11. Журнал «Сети» // URL: http://www.osp.ru/nets.
12. Журнал «Computerworld» // URL: http://www.osp.ru/cw.
13. Журнал «LAN» // URL: URL: http://www.osp.ru/lan /+электронный ресурс/.
14. Издательство “Открытые системы” // URL: http://www.osp.ru.
15. Официальный сайт компании Microsoft // URL: http://www.microsoft.com.
16. ПО для организации конференций
17. СПС «КонсультантПлюс» // URL: http://www.consultant.ru/document/cons_doc
18. СПС «ГАРАНТ» // URL: http://base.garant.ru/
19. ЦИТ Форум // URL: http://citforum.ru.
20. ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. // URL: http://base.garant.ru/12148555/

Раздел 7. Материально-техническая база и информационные технологии

Материально-техническое обеспечение дисциплины «**Информационная безопасность**» включает в себя учебные аудитории для проведения лекционных, практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы обучающихся.

Учебные аудитории укомплектованы специализированной мебелью и техническими средствами обучения. Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети Интернет.

Дисциплина может реализовываться с применением дистанционных технологий обучения. Специфика реализации дисциплины с применением дистанционных технологий обучения устанавливается дополнением к рабочей программе. В части не противоречащей специфике, изложенной в дополнении к программе, применяется настоящая рабочая программа.

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине с применением дистанционных образовательных технологий включает в себя:
Компьютерная техника, расположенная в учебном корпусе Института (ул.Качинцев, 63, кабинет Центра дистанционного обучения):

1) Intel i 3 3.4Ghz\ОЗУ 4Gb\500GB\RadeonHD5450
2) Intel PENTIUM 2.9GHz\ОЗУ 4GB\500GB
3) личные электронные устройства (компьютеры, ноутбуки, планшеты и иное), а также средства связи преподавателей и студентов.

Информационные технологии, необходимые для осуществления образовательного процесса по дисциплине с применением дистанционных образовательных технологий включают в себя:

- система дистанционного обучения (СДО) (Learning Management System) (LMS) Moodle (Modular Object-Oriented Dynamic Learning Environment);
- электронная почта;
- система компьютерного тестирования;
- электронная библиотека IPRbooks;
- система интернет-связи skype;
- телефонная связь;
- ПО для организации конференций

Обучение обучающихся инвалидов и обучающихся с ограниченными возможностями здоровья осуществляется посредством применения специальных технических средств в зависимости от вида нозологии.

При проведении учебных занятий по дисциплине используются мультимедийные комплексы, электронные учебники и учебные пособия, адаптированные к ограничениям здоровья обучающихся.

Лекционные аудитории оборудованы мультимедийными кафедрами, подключенными к звуковым колонкам, позволяющими усилить звук для категории слабослышащих обучающихся, а также проекционными экранами которые увеличивают изображение в несколько раз и позволяют воспринимать учебную информацию обучающимся с нарушениями зрения.

При обучении лиц с нарушениями слуха используется усилитель слуха для слабослышащих людей Cyber Ear модель HAP-40, помогающий обучаемым лучше воспринимать учебную информацию.

Обучающиеся с ограниченными возможностями здоровья, обеспечены печатными и электронными образовательными ресурсами (программы, учебники, учебные пособия, материалы для самостоятельной работы и т.д.) в формах, адаптированных к ограничениям их здоровья и восприятия информации:

для лиц с нарушениями зрения:

- в форме электронного документа;
- в форме аудиофайла;

для лиц с нарушениями слуха:

- в печатной форме;

- в форме электронного документа;

для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Программное обеспечение, используемое на занятиях**:**

- Операционная система Windows,
- Архиватор 7-zip,
- Система тестирования,
- Microsoft Office 2007,
- Антивирус Касперский 6,
- Консультант+,
- Виртуальная машина VirtualBox,
- Виртуальная машина VirtualPC,
- Internet Explorer.

Раздел 8. Методические указания для обучающихся по освоению дисциплины

Для успешного усвоения материала курса требуются значительное время, концентрация внимания и усилия: посещение лекционных занятий и конспектирование преподаваемого материала, работа с ним дома, самостоятельная проработка материала рекомендуемых учебников и учебных пособий при самостоятельной подготовке. Особое внимание следует обратить на выполнение практических работ, практических заданий по СРО, тестовых вопросов.

При самостоятельной работе с учебниками и учебными пособиями полезно иметь под рукой справочную литературу (энциклопедии) или доступ к сети Интернет, так как могут встречаться новые термины, понятия, которые раньше обучающиеся не знали.

Цель практических занятий по дисциплине «Информационная безопасность» - закрепление знаний по определенной теме, приобретенных в результате прослушивания лекций, получения консультаций и самостоятельного изучения различных источников литературы. При выполнении данных работ обучающиеся должны будут глубоко изучить методы и методики обеспечения информационной безопасности. Получить навыки настройки и обслуживания антивирусного программного обеспечения.

Перед практическим занятием обучающийся должен детально изучить теоретические материалы вопросов практики в учебниках, конспектах лекций, периодических журналах и прочее. Если при выполнении практического задания у обучающегося остаются неясности, то ему необходимо оперативно обратиться к преподавателю за уточнением.

После выполнения практического задания обучающиеся должны выполнить самостоятельную работу. Самостоятельная работа включает в себя индивидуальное задание по пройденной теме. Таким образом, каждый обучающийся выполняет только свой вариант задания. Выполнение практических заданий сопровождается выполнением письменного отчета в тетради. Отчет должен выполняться аккуратно, быть легко читаемым подчерком, при этом допускаются общепринятые сокращения.

При дистанционном выполнении практических работ, обучающийся может самостоятельно приобрести операционные системы Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10. Ответственность за установку и настройку программного обеспечения в данном случае ложится на обучающегося. Следует воспользоваться методическими указаниями по установке данных программных систем.

Результаты выполненных заданий оцениваются с учетом теоретических знаний по соответствующим разделам дисциплины, техники выполнения работы, объективности и обоснованности принимаемых решений в процессе работы с данными, качества оформления. Переход к выполнению следующего практического задания допускается только после отчета выполненной работы.

Учебно-методическое издание

Рабочая программа учебной дисциплины

Информационная безопасность

(Наименование дисциплины в соответствии с учебным планом)

Филиппов Михаил Владимирович

(Фамилия, Имя, Отчество составителя)