МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ»
(КНИТУ-КАИ)
Чистопольский филиал «Восток»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ЛАБОРАТОРНЫМ РАБОТАМ

по дисциплине

ЗАЩИТА ИНФОРМАЦИИ

Индекс по учебному плану: **Б1.О.16**

Направление подготовки: **09.03.01 Информатика и вычислительная техника**

Квалификация: **Бакалавр**

Профиль подготовки: **Вычислительные машины, комплексы, системы и сети**

Типы задач профессиональной деятельности: **проектный, производственно-технологический**

Рекомендовано УМК ЧФ КНИТУ-КАИ

Чистополь
2023 г.

Лабораторная работа № 1

Подсистемы парольной аутентификации пользователей. Генераторы паролей. Оценка степени стойкости парольной защиты

Под идентификацией пользователя понимают присвоение ему некоторого несекретного идентификатора, который он должен предъявить СЗИ при осуществлении доступа к объекту. В качестве идентификатора может быть использован, например, login, физическое устройство, и т.д.

Под аутентификацией понимают подтверждение пользователем своего идентификатора, проверка его подлинности. Данный этап необходим для устранения фальсификации идентификатора, предотвращения несанкционированного доступа в случае утери пользователем идентификатора.

Подсистемы идентификации и аутентификации пользователя играют очень важную роль для систем защиты информации.

Стойкость подсистемы идентификации и аутентификации пользователя в системе защиты информации (СЗИ) во многом определяет устойчивость к взлому самой СЗИ. Данная стойкость определяется гарантией того, что злоумышленник не сможет пройти аутентификацию, присвоив чужой идентификатор или украв его.

Парольные системы идентификации/аутентификации является одними из основных и наиболее распространенных в СЗИ методами пользовательской аутентификации в силу их простоты и прозрачности. В данном случае, информацией, аутентифицирующей пользователя, является некоторый секретный пароль, известный только легальному пользователю.

Парольная аутентификация пользователя является, как правило, передним краем обороны СЗИ. В связи с этим, модуль аутентификации по паролю наиболее часто подвергается атакам со стороны злоумышленника. Цель злоумышленника в данном случае – подобрать аутентифицирующую информацию (пароль) легального пользователя.

Методы парольной аутентификации пользователя являются наиболее простыми методами аутентификации и при несоблюдении определенных требований к выбору пароля являются достаточно уязвимыми.

Основными минимальными требованиями к выбору пароля и к подсистеме парольной аутентификации пользователя являются следующие.

К паролю

1. Минимальная длина пароля должна быть не менее 6 символов.

2. Пароль должен состоять из различных групп символов (малые и большие латинские буквы, цифры, специальные символы ‘(’, ‘)’, ‘#’ и т.д.).

3. В качестве пароля не должны использоваться реальные слова, имена, фамилии и т.д.

К подсистеме парольной аутентификации.

1. Администратор СЗИ должен устанавливать максимальный срок действия пароля, после чего, он должен быть сменен.

2. В подсистеме парольной аутентификации должно быть установлено ограничение числа попыток ввода пароля (обычно, не более 3).

3. В подсистеме парольной аутентификации должна быть установлена временная задержка при вводе неправильного пароля.

Как правило, для помощи администратору безопасности в формировании паролей подчиненных ему пользователей, удовлетворяющих перечисленным требованиям к паролям, используются особые программы - автоматические генераторы паролей пользователей.

При выполнении перечисленных требований к паролям и к подсистеме парольной аутентификации, единственно возможным методом взлома данной подсистемы злоумышленником является прямой перебор паролей (brute forcing). В данном случае, количественная оценка стойкости парольной защиты осуществляется следующим образом.

Количественная оценка стойкости парольной защиты

Пусть A – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля. Например, если пароль состоит только из малых английских букв, то A=26).

L – длина пароля.

$S = A^L$ - число всевозможных паролей длины L, которые можно составить из символов алфавита A.

V – скорость перебора паролей злоумышленником.

T – максимальный срок действия пароля.

Тогда, вероятность P подбора пароля злоумышленником в течении срока его действия V определяется по следующей формуле.

$$P = \frac{V * T}{S} = \frac{V * T}{A^L}$$

Эту формулу можно использовать в обратную сторону для решения следующей задачи:

ЗАДАЧА. Определить минимальные мощность алфавита паролей A и длину паролей L, обеспечивающих вероятность подбора пароля злоумышленником не более заданной P, при скорости подбора паролей V, максимальном сроке действия пароля T.

Данная задача имеет неоднозначное решение. При исходных данных V,T,P однозначно можно определить лишь нижнюю границу S^* числа всевозможных паролей. Целочисленное значение нижней границы вычисляется по следующей формуле

$$S^* = \left\lceil \frac{V * T}{P} \right\rceil \qquad (1)$$

где $\lceil\ \rceil$ - целая часть числа, взятая с округлением вверх.

После нахождения нижней границы S^* необходимо выбрать такие A и L для формирования $S=A^L$, чтобы выполнялось неравенство (2).

$$S^* \le S = A^L \qquad (2)$$

При выборе S, удовлетворяющего неравенству (2), вероятность подбора пароля злоумышленника (при заданных V и T) будет меньше, чем заданная P.

Необходимо отметить, что при осуществлении вычислений по формулам (1) и (2), величины должны быть приведены к одним размерностям.

Пример

Исходные данные – $P=10^{-6}$, T=7 дней = 1 неделя, V=10 паролей / минуту = 10*60*24*7=100800 паролей в неделю.

Тогда, $S^* = \left[\frac{100800 * 1}{10^{-6}} \right] = 1008 * 10^8$.

Условию $S^* \le A^L$ удовлетворяют, например, такие комбинации A и L, как A=26, L=8 (пароль состоит из 8 малых символов английского алфавита), A=36, L=6 (пароль состоит из 6 символов, среди которых могут быть малые латинские буквы и произвольные цифры).

Задание на лабораторную работу

1. В таблице 1 найти для вашего варианта значения характеристик P,V,T, а также группы символов, используемых при формировании пароля.

2. Вычислить мощность алфавита паролей A, соответствующую Вашему варианту.

3. Вычислить по формуле (1) нижнюю границу S^* для заданных P,V,T.

4. Зная мощность алфавита паролей A, вычислить минимальную длину пароля L, при котором выполняется условие (2).

5. Реализовать на языке программирования программу, реализующую генератор паролей с характеристиками, соответствующими Вашему варианту. Программа должна формировать случайную последовательность символов длины L, должны использоваться символы из тех групп, которые выданы Вашему варианту.

Замечания: При реализации программы могут быть полезны следующие коды символов

Коды английских символов : «A»=65,…,«Z»=90, «a»=97,…, «z» =122.

Коды цифр : «0» = 48, «9» = 57.

! - 33, “ – 34, # - 35, $ - 36, % - 37, & - 38, ‘ – 39, (- 40,) – 41, * - 42.

Коды русских символов : «А» - 128, … «Я» - 159, «а» - 160,…, «п» - 175, «р» - 224,…, «я» - 239.

Контрольные вопросы

1. Что понимается под идентификацией и аутентификацией пользователя?

2. Чем определяется стойкость к взлому подсистемы идентификации и аутентификации пользователя?

3. Перечислите основные требования к выбору пароля и к реализации подсистемы парольной аутентификации пользователя.

4. Как количественно оценить стойкость подсистемы парольной аутентификации к взлому?

5. Как изменится стойкость к взлому подсистемы парольной аутентификации при увеличении характеристик *P*,*V*,*T*? При их уменьшении?

Вариант	*P*	*V*	*T*	*Используемые группы символов пароля*
1	10^{-4}	15 паролей/мин	2 недели	1. Цифры (0-9) 2. Латинские строчные буквы (a-z)
2	10^{-5}	3 паролей/мин	10 дней	1. Латинские прописные буквы (A-Z) 2. Русские строчные буквы (а-я)
3	10^{-6}	10 паролей/мин	5 дней	1. Русские прописные буквы (А-Я) 2. Специальные символы.
4	10^{-7}	11 паролей/мин	6 дней	1. Цифры (0-9) 2. Латинские прописные буквы (A-Z)
5	10^{-4}	100 паролей/день	12 дней	1. Русские прописные буквы (А-Я) 2. Латинские строчные буквы (a-z)
6	10^{-5}	10 паролей/день	1 месяц	1. Русские строчные буквы (а-я) 2. Специальные символы.
7	10^{-6}	20 паролей/мин	3 недели	1. Цифры (0-9) 2. Русские строчные буквы (а-я)
8	10^{-7}	15 паролей/мин	20 дней	1. Латинские строчные буквы (a-z) 2. Латинские прописные буквы (A-Z)
9	10^{-4}	3 паролей/мин	15 дней	1. Русские прописные буквы (А-Я) 2. Русские строчные буквы (а-я)
10	10^{-5}	10 паролей/мин	1 неделя	1. Цифры (0-9) 2. Специальные символы.
11	10^{-6}	11 паролей/мин	2 недели	1. Цифры (0-9) 2. Русские прописные буквы (А-Я)
12	10^{-7}	100 паролей/день	10 дней	1. Латинские строчные буквы (a-z) 2. Русские прописные буквы (А-Я)
13	10^{-4}	10 паролей/день	5 дней	1. Цифры (0-9)

				2. Латинские строчные буквы (a-z)
14	10^{-5}	20 паролей/мин	6 дней	1. Латинские прописные буквы (A-Z) 2. Русские строчные буквы (а-я)
15	10^{-6}	15 паролей/мин	12 дней	1. Русские прописные буквы (А-Я) 2. Специальные символы.
16	10^{-7}	3 паролей/мин	1 месяц	1. Цифры (0-9) 2. Латинские прописные буквы (A-Z)
17	10^{-4}	10 паролей/мин	3 недели	1. Русские прописные буквы (А-Я) 2. Латинские строчные буквы (a-z)
18	10^{-5}	11 паролей/мин	20 дней	1. Русские строчные буквы (а-я) 2. Специальные символы.
19	10^{-6}	100 паролей/день	15 дней	1. Цифры (0-9) 2. Русские строчные буквы (а-я)
20	10^{-7}	10 паролей/день	1 неделя	1. Латинские строчные буквы (a-z) 2. Латинские прописные буквы (A-Z)
21	10^{-4}	20 паролей/мин	2 недели	1. Русские прописные буквы (А-Я) 2. Русские строчные буквы (а-я)
22	10^{-5}	15 паролей/мин	10 дней	1. Цифры (0-9) 2. Специальные символы.
23	10^{-6}	3 паролей/мин	5 дней	1. Цифры (0-9) 2. Русские прописные буквы (А-Я)
24	10^{-7}	10 паролей/мин	6 дней	1. Латинские строчные буквы (a-z) 2. Русские прописные буквы (А-Я)
25	10^{-4}	11 паролей/мин	12 дней	1. Цифры (0-9) 2. Латинские строчные буквы (a-z)
26	10^{-5}	100 паролей/день	1 месяц	1. Латинские прописные буквы (A-Z) 2. Русские строчные буквы (а-я)
27	10^{-6}	10 паролей/день	3 недели	1. Русские прописные буквы (А-Я) 2. Специальные символы.
28	10^{-7}	20 паролей/мин	20 дней	1. Цифры (0-9) 2. Латинские прописные буквы (A-Z)
29	10^{-4}	15 паролей/мин	15 дней	1. Русские прописные буквы (А-Я) 2. Латинские строчные буквы (a-z)
30	10^{-5}	3 паролей/мин	1 неделя	1. Русские строчные буквы (а-я) 2. Специальные символы.

Лабораторная работа № 2

Реализация политик информационной безопасности. Дискреционная модель политики безопасности

Цель – изучение проблемам реализации политик информационной безопасности в компьютерных системах на примере дискреционной модели.

Политики безопасности

Под политикой безопасности понимается набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации. Политика безопасности задает механизмы управления доступа к объекту, определяет как разрешенные, так и запрещенные типы доступов, регламентирует поведение СЗИ в различных ситуациях.

При выборе и реализации политики безопасности в компьютерной системе, как правило, работают следующие шаги:

1. В информационную структуру вносится структура ценностей (определяется ценность информации) и проводится анализ угроз и рисков для информации и информационного обмена.
2. Определяются правила использования для любого информационного процесса, права доступа к элементам информации с учетом данной оценки ценностей.

Реализация политики безопасности должна быть четко продумана. Результатом ошибочного или бездумного определения правил политики безопасности, как правило, является разрушение ценности информации без нарушения политики.

Существует ряд моделей политик безопасности, отличающихся по возможностям защиты, по качеству защиты, по особенностям реализации. Одной из самых простых и распространенных моделей политик безопасности является дискреционная политика.

Дискреционная политика безопасности

Пусть O – множество объектов компьютерной системы, над которыми могут производиться различные операции, U – множество пользователей (субъектов) компьютерной системы, которые могут производить операции над объектами, S – множество всевозможных операций (действий) субъектов над объектами.

Дискреционная политика безопасности определяет отображение $O \to U$ (объектов на пользователей-субъектов). В соответствии с данным отображением, каждый объект $O_j \in O$ объявляется собственностью соответствующего пользователя $U_k \in U$, который может выполнять над ними определенную совокупность действий $S_i \subset S$, в которую могут входить несколько элементарных действий (чтение, запись, модификация и т.д.). Пользователь, являющийся собственником объекта, иногда имеет право передавать часть или все права другим пользователям (обладание администраторскими правами).

Указанные права доступа пользователей-субъектов к объектам компьютерной системы записываются в виде так называемой МАТРИЦЫ ДОСТУПОВ. На пересечении *i*-ой строки и *j*-ого столбца данной матрицы располагается элемент S_{ij} – множество разрешенных действий *j*-ого субъекта над *i*-ым объектом.

Пример

Пусть имеем множество из 3 пользователей-субъектов O={Администратор, Гость, Пользователь_1} и множество из 4 объектов U={Файл_1, Файл_2, CD-RW, Флоппи-Дисковод}.

Пусть множество возможных действий включает следующие: S={Чтение, Запись, Передача прав}. Кроме этого, существует два дополнительных типа операций - «Полные права», «Полный запрет». Действие «Полные права» разрешает выполнение всех из перечисленных 3 действий, «Полный запрет» запрещает выполнение всех из вышеперечисленных действий. Право «Передача прав» позволяет передавать субъекту свои права на объект другому субъекту.

В данном случае, матрица доступа, описывающая дискреционную политику безопасности, может выглядеть, например, следующим образом.

Таблица 1

Объект / Субъект	Файл_1	Файл_2	CD-RW	Флоппи-дисковод
Администратор	Полные права	Полные права	Полные права	Полные права
Гость	Запрет	Чтение	Чтение	Запрет
Пользователь_1	Чтение, передача прав	Чтение, запись	Полные права	Полный запрет

Например, Пользователь_1 имеет права на чтение и запись в Файл_2.

Пользователь_1 может передать свое право на чтение из Файла_1 другому пользователю. Если Пользователь_1 передает право на чтение к Файлу_1 пользователю Гость, то у пользователя Гость появляется право чтения из Файла_1, соответственно модифицируется матрица доступов.

Порядок выполнения работы

Пусть множество S возможных операций субъектов над объектами компьютерной системы задано в виде: S = {«Доступ на чтение», «Доступ на запись», «Передача прав»}.

1. Получите из таблицы 2 информацию о количестве субъектов и объектов компьютерной системы, соответственно Вашему варианту.

2. Реализуйте программный модуль, формирующий матрицу доступов субъектов к объектам компьютерной системы в виде, аналогичном таблице 1. Реализация данного модуля подразумевает реализацию следующих шагов:

2.1. Выбрать идентификаторы пользователей, которые будут использоваться при их входе в компьютерную систему (по одному идентификатору для каждого пользователя, количество пользователей задано для Вашего варианта). Например, множество из 3 идентификаторов пользователей {Ivan, Sergey, Boris}. Один из данных идентификаторов должен соответствовать администратору компьютерной системы (пользователю, обладающему полными правами ко всем объектам).

2.2. Создать и случайным образом заполнить матрицу доступа субъектов к объектам в виде, аналогичном таблице 1. При заполнении матрицы учесть следующее:

2.2.1. Один из пользователей-субъектов должен являться администратором системы. Для него права доступа ко всем объектам системы должны быть выставлены как полные.

2.2.2. Пользователь может иметь несколько прав доступа к некоторому объекту компьютерной системы, иметь полные права, либо совсем не иметь прав.

Замечание по реализации

Для реализации программной модели матрицы доступов можно использовать массив размерности M x N, где M – количество субъектов, N – количество объектов.

Права доступов в ячейках матрицы доступов можно кодировать трехбитными числами от 0 до 7, например, в следующем виде:

Бит доступа по чтению	Бит доступа по записи	Бит передачи прав

Тогда, соответствие множеств типов доступов и соответствующих значений в матрице доступов будет следующее:

Десятичное число	**Двоичное число**	**Разрешенные типы доступов**
0	000	Полный запрет
1	001	Передача прав
2	010	Запись
3	011	Запись, Передача прав
4	100	Чтение
5	101	Чтение, Передача прав
6	110	Чтение, Запись
7	111	Полный доступ

3. Реализовать программный модуль, демонстрирующий работу пользователя в дискреционной модели политики безопасности. Данный модуль должен выполнять следующие функции:

3.1. При запуске модуля должен запрашиваться идентификатор пользователя (должна проводиться идентификация пользователя). В случае успешной идентификации пользователя должен осуществляться вход в систему, в случае неуспешной – выводиться соответствующее сообщение.

3.2. При входе в систему после успешной идентификации пользователя, на экране должен распечатываться список всех объектов системы с указанием перечня всех доступных прав доступа идентифицированного пользователя к данным объектам. Вывод можно осуществить, например, следующим образом:

User: Boris

Идентификация прошла успешно, добро пожаловать в систему

Перечень Ваших прав:

Объект1: Чтение

Объект2: Запрет

Объект3: Чтение, Запись

Объект4: Полные права

Жду ваших указаний >

3.3. После вывода на экран перечня прав доступа пользователя к объектам компьютерной системы, программа должна ждать указаний пользователя на осуществление действий над объектами в компьютерной системе. После получения команды от пользователя, на экран должно выводиться сообщение об успешности либо не успешности операции. При выполнении операции передачи прав (grant), должна модифицироваться матрица доступов. Должна поддерживаться операция выхода из системы (quit), после которой должен запрашиваться другой идентификатор пользователя. Диалог можно организовать, например, следующим образом:

Жду ваших указаний > read

Над каким объектом производится операция? 1

Операция прошла успешно

Жду ваших указаний > write

Над каким объектом производится операция? 2

Отказ в выполнении операции. У Вас нет прав для ее осуществления

Жду ваших указаний > grant

Право на какой объект передается? 3

Отказ в выполнении операции. У Вас нет прав для ее осуществления

Жду ваших указаний > grant

Право на какой объект передается? 4

Какое право передается? read

Какому пользователю передается право? Ivan

Операция прошла успешно

Жду ваших указаний > quit

Работа пользователя Boris завершена. До свидания.

User:

Замечание по реализации

Для контроля возможности заданного типа доступа в рамках предложенной выше программной модели необходимо проверить равенство единице соответствующего бита числа в ячейке матрицы доступов. Для этого можно воспользоваться свойствами операций целочисленного деления я взятия остатка от деления на 2.

Для того, чтобы проверить равенство n-го бита некоторого числа на равенство единице необходимо целочисленно поделить это число на 2^{n-1} и проверить на нечетность получившееся число. Если после деления получили нечетное число, то n-ый бит исходного числа равен единице, иначе – равен нулю.

Пример

Проверить возможность доступа по записи Пользователя_2 к Файлу_3.

1. Берем элемент матрицы доступов, находящийся на пересечении второй строки и третьего столбца. Пусть этот элемент равен 3.

2. Для контроля возможности доступа по чтению, необходимо проверить равенство второго бита числа на единицу. Для этого целочисленно поделим число 3 на $2^{2-1}=2$.

3. $\left[\frac{3}{2}\right]=1$ - число нечетное, то есть второй бит числа 3 равен единице, то есть доступ по записи Пользователя_2 к Файлу_3 разрешен.

4. Протестировать реализованную программу, продемонстрировав реализованную модель дискреционной политики безопасности преподавателю.

Контрольные вопросы

1. Что понимается под политикой безопасности в компьютерной системе?
2. В чем заключается модель дискреционной политики безопасности в компьютерной системе?
3. Что понимается под матрицей доступа в дискреционной политике безопасности? Что хранится в данной матрице?
4. Какие действия производятся над матрицей доступа в том случае, когда один субъект передает другому субъекту свои права доступа к объекту компьютерной системы?

Таблица 2

Вариант	Количество субъектов доступа (пользователей)	Количество объектов доступа
1	5	5
2	4	4
3	5	4
4	6	5
5	7	6
6	8	3
7	9	4
8	10	4
9	3	5
10	4	6
11	5	3
12	6	4
13	7	4
14	8	5
15	9	6
16	10	3
17	3	4
18	4	4
19	5	5
20	6	6
21	7	3
22	8	4
23	9	4
24	10	5
25	3	6
26	4	3
27	5	4
28	6	4
29	6	5
30	8	6

Лабораторная работа № 3

Мандатные политики безопасности. Политика безопасности Белла-ЛаПадулы

Цель работы – изучить мандатные модели политик безопасности, а также особенности их реализации. Изучить основные достоинства и недостатки данных моделей. Познакомиться с проблемой системы Z.

Политики безопасности

Под политикой безопасности понимается набор норм, правил и практических рекомендаций, которые регулируют управление, защиту и распределение ценной информации. Политика безопасности задает механизмы управления доступа к объекту, определяет как разрешенные, так и запрещенные типы доступов, регламентирует поведение СЗИ в различных ситуациях.

Реализация политики безопасности должна быть четко продумана. Результатом ошибочного или бездумного определения правил политики безопасности, как правило, является разрушение ценности информации без нарушения политики.

Существует ряд моделей политик безопасности, отличающихся по возможностям защиты, по качеству защиты, по особенностям реализации. Базовыми политиками безопасности в компьютерных системах являются дискреционная и мандатная политики безопасности.

Исходная мандатная политика безопасности

Пусть в компьютерной системе определено множество субъектов доступа $S = \{S_i\}_{i=\overline{1,n}}$ и множество объектов доступа $O = \{O_j\}_{j=\overline{1,m}}$.

Исходная мандатная политика управления доступом (*Mandatory Access*) в компьютерной системе базируется на следующей группе аксиом.

1. Вводится множество атрибутов безопасности *A*, элементы которого упорядочены с помощью установленного отношения доминирования. Например, для России характерно использование следующего множества уровней безопасности *A*={открыто (О), конфиденциально (К), секретно (С), совершенно секретно (СС), особая важность (ОВ)}.

2. Каждому объекту $O_j \in O$ компьютерной системы ставится в соответствие атрибут безопасности $x_{O_j} \in A$, который соответствует ценности объекта O_j и называется его *уровнем (грифом) конфиденциальности*.

3. Каждому субъекту $S_i \in S$ компьютерной системы ставится в соответствие атрибут безопасности $x_{S_i} \in A$, который называется *уровнем допуска* субъекта и равен максимальному из уровней конфиденциальности объектов, к которому субъект S_i будет иметь допуск.

4. Если субъект S_i имеет уровень допуска x_{S_i}, а объект O_j имеет уровень конфиденциальности x_{O_j}, то S_i будет иметь допуск к O_j тогда и только тогда, когда $x_{S_i} \geq x_{O_j}$.

Пример 1

Пусть в компьютерной системе задано множество из 4 субъектов доступа S={Administrator, User1, User2, Guest} и множество из 5 объектов O={FILE1.DAT, FILE2.TXT, FILE3.TXT, CD-ROM, FDD}. Множество атрибутов безопасности A компьютерной системы определено как A={NONCONFIDENTIAL, CONFIDENTIAL, SECRET, TOP SECRET}.

Пусть уровни конфиденциальности объектов определены следующим образом:

FDD – NONCONFIDENTIAL.

CD-ROM – CONFIDENTIAL.

FILE1.DAT – SECRET.

FILE2.TXT – SECRET.

FILE3.TXT – TOP SECRET.

Пусть уровни допуска субъектов определены следующим образом:

Administrator – TOP SECRET.

User1 – SECRET.

User2 – CONFIDENTIAL.

Guest – NONCONFIDENTIAL.

Тогда,

субъект Administrator будет иметь допуск ко всем объектам;

субъект User1 будет иметь допуск к объектам FDD, CD-ROM, FILE1.DAT, FILE2.DAT;

субъект User2 будет иметь допуск к объектам FDD, CD-ROM;

субъект Guest будет иметь допуск только к объекту FDD.

Основной недостаток исходной мандатой политики безопасности – возможность утечки информации сверху вниз, например, с помощью реализации «троянских коней», запускаемых с максимальными привилегиями и способных записывать информацию на нижние уровни, откуда ее могут считать пользователи с меньшими привилегиями.

Представленный недостаток отчасти решается в политике безопасности Белла-ЛаПадула.

Мандатная модель политики безопасности Белла-ЛаПадула (БЛМ)

Модель БЛМ базируется на 2 свойствах безопасности.

Первое свойство аналогично исходной мандатной модели политики безопасности.

Свойство NRU (not read up) - «нет чтения вверх», гласит, что субъект S_i, имеющий уровень допуска x_{S_i}, может читать информацию из объекта O_j с уровнем безопасности x_{O_j}, только если $x_{O_j} \leq x_{S_i}$.

Второе свойство модели БЛМ позволяет отчасти решить проблему утечки информации сверху вниз.

Свойство (NWD) (not write down) - «нет записи вниз», гласит, что субъект S_i, имеющий уровень допуска x_{S_i}, может записывать информацию в объект O_j с уровнем безопасности x_{O_j}, только если $x_{O_j} \geq x_{S_i}$.

Введение свойства NWD разрешает проблему троянских коней, так как запись информации на более низкий уровень безопасности, типичная для троянских коней, запрещена.

В политике Белла-ЛаПадула субъект может понизить свой уровень допуска по своему желанию, а также повысить его до изначально ему назначенного администратором компьютерной системы.

Пример 2

Рассмотрим пример компьютерной системы, а также грифов конфиденциальности и уровней допуска, введенных в примере 1.

При ее реализации в рамках политики БЛМ возможно выполнение следующих операций:

1. субъект Administrator будет иметь допуск по чтению из всех объектов, и допуск по записи в объект FILE3.TXT;
2. субъект User1 будет иметь допуск по чтению из объектов FDD, CD-ROM, FILE1.DAT, FILE2.DAT и допуск по записи в объекты FILE1.DAT, FILE2.TXT, FILE3.TXT;
3. субъект User2 будет иметь допуск по чтению из объектов CD-ROM, FDD и допуск по записи в объекты FILE1.DAT, FILE2.TXT, FILE3.TXT, CD-ROM;
4. субъект Guest будет иметь допуск по чтению из объекта FDD и допуск по записи во все объекты.

Кроме этого, например, субъект User1 может понизить свой уровень допуска с SECRET до CONFIDENTIAL и восстановить его обратно до SECRET.

Проблема системы Z

Основным недостатком модели БЛМ считается возможность реализации так называемой системы Z, когда некий пользователь с высокими привилегиями по незнанию (либо завербованный) может рассекретить часть доступной ему информации, записав ее в объекты с более низким уровнем конфиденциальности.

Допустим, субъект S_i с уровнем допуска x_{S_i} читает информацию из объекта, уровень конфиденциальности которого также равен x_{S_i}. Далее, данный субъект понижает свой уровень допуска до уровня x_{O_j} ($x_{O_j} < x_{S_i}$). После этого, он может записать информацию в объект с классификацией x_{O_j}. Нарушения БЛМ формально не произошло, но безопасность системы нарушена.

Для устранения данного недостатков, в модели БЛМ вводят правила сильного и слабого спокойствия.

Реализация и исследование политики безопасности Белла-ЛаПадула.

Пусть множество возможных операций субъектов *S* над объектами *O* задано в следующей форме: {«READ (доступ по чтению)», «WRITE (доступ по записи)», «CHANGE (изменение уровня доступа субъекта)»}.

Пусть множество атрибутов безопасности *A* задано в виде *A*={NONCONFIDENTIAL, CONFIDENTIAL, SECRET, TOP SECRET}.

1. Получите из таблицы 1 информацию о количестве субъектов и объектов компьютерной системы соответственно Вашему варианту.

2. Реализовать программный модуль, формирующий политику безопасности Белла-ЛаПадулы.

2.1. Выбрать идентификаторы пользователей, которые будут использоваться при их входе в компьютерную систему (по одному идентификатору для каждого пользователя, количество пользователей задано для Вашего варианта). Например, множество из 3 идентификаторов пользователей {Admin, User1, User2}. Один из данных идентификаторов должен соответствовать администратору компьютерной системы, обладающему максимальными правами доступа.

2.2. Случайным образом присвоить объектам компьютерной системы уровни конфиденциальности из множества *A*.

2.3. Случайным образом присвоить субъектам компьютерной системы уровни допуска из множества *A*. Учесть, что один из данных субъектов будет являться администратором, обладающим максимальным уровнем допуска.

Замечания по реализации

1. Для кодирования в программной модели атрибутов безопасности множества A можно закодировать их числами от 0 до 3 (от низших к высшим уровням безопасности), например, NONCONFIDENTIAL=0, CONFIDENTIAL=1, SECRET=2, TOP SECRET=3. В этом случае более легко можно реализовать контроль допуска субъектов к объектам.

2. Для хранения в программной модели уровней конфиденциальности объектов и уровней допуска субъектов рекомендуется использовать два массива,

которые должны заполняться случайным образом (за исключением уровня допуска администратора).

3. Необходимо хранить копию начальных уровней доступа субъектов для контроля их не превышения в результате выполнения операции change.

3. Реализовать программный модуль, демонстрирующий работу пользователя в мандатной модели политики безопасности. Данный модуль должен выполнять следующие функции:

3.1. При запуске модуля – распечатать на экране сформированную модель БЛМ – уровни конфиденциальности объектов и уровни допуска субъектов.

3.2. Запрос идентификатора пользователя (должна проводиться его идентификация). В случае успешной идентификации пользователя должен осуществляться вход в систему, в случае неуспешной – выводиться соответствующее сообщение.

Возможный пример работы модуля с реализацией функций п. 3.1. и 3.2. представлен ниже.

OBJECTS:
Object 1 : NONCONFIDENTIAL
Object 2 : CONFIDENTIAL
Object 3 : TOP_SECRET
SUBJECTS:
Administrator : TOP_SECRET
User1 : SECRET
User2 : NONCONFIDENTIAL
Login: User1
Command>

3.3. По результатам идентификации субъекта после входа в систему, программа должна ждать указаний пользователя на осуществление действий над объектами в компьютерной системе. После получения команды от пользователя, на экран должно выводиться сообщение об успешности либо не успешности

операции. При выполнении операции изменения уровня доступа субъекта (change) данный уровень должен модифицироваться. Должна поддерживаться операция выхода из системы (exit), после которой, на экран вновь должна выводиться информация об уровнях доступа субъектов и уровнях конфиденциальности объектов и запрашиваться другой идентификатор пользователя. Диалог можно организовать, например, следующим образом (для выше построенного примера модели БЛМ):

Login: Administrator
command> read
At what object? 1
Read success
Command> write
At what object? 1
Write denied
Command> write
At what object? 3
Write success
Command> change
Enter CLASSIFICATION : NONCONFIDENTIAL
Administrator is NONCONFIDENTIAL
Command> write
At what object? 1
Write success
Command> change
Enter CLASSIFICATION : TOP_SECRET
Administrator is TOP_SECRET

4. Протестировать реализованную модель политики безопасности БЛМ в различных ситуациях и продемонстрировать ее преподавателю.

5. Продемонстрировать возможность реализации системы Z в разработанной модели БЛМ.

Контрольные вопросы

1. Что понимают под политикой безопасности?
2. Перечислить группу аксиом, определяющих базовую мандатную политику безопасности. Что понимают под уровнем конфиденциальности и уровнем допуска?
3. В чем заключается основной недостаток базовой мандатной политики безопасности?
4. Как определяется политика безопасности Белла-ЛаПадула? В каких случаях разрешены операции read, write, change в данной политике?
5. В чем заключается проблема системы Z? Показать и прокомментировать в сформированном отчете группу команд, реализующих систему Z.

Табл. 3. Варианты

Вариант	Количество субъектов доступа (пользователей)	Количество объектов доступа
1	4	4
2	4	6
3	5	4
4	6	5
5	7	6
6	8	3
7	9	4
8	10	4
9	4	5
10	4	6
11	5	3
12	6	4
13	7	4
14	8	5
15	9	6
16	10	3
17	4	5
18	4	4
19	5	5
20	6	6
21	7	3
22	8	4
23	9	4
24	10	5
25	3	6
26	4	3
27	5	4
28	6	4
29	6	5
30	8	6

Лабораторная работа № 4

Методы криптографической защиты информации

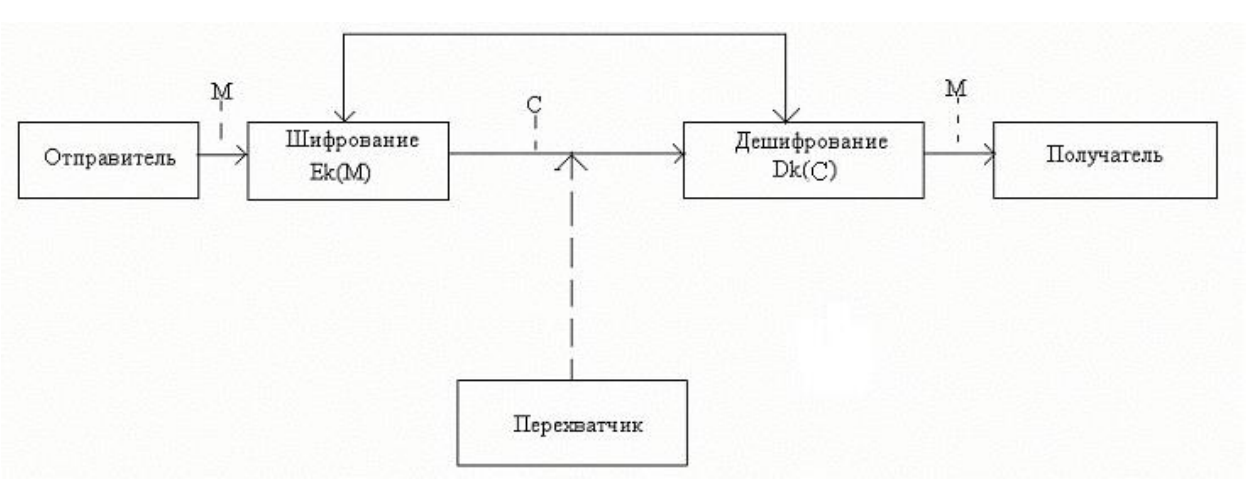
Простейшие алгоритмы шифрования

Цель работы – изучение простейших традиционных алгоритмов криптографической защиты информации и особенностей их практической реализации.

Криптография

Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для противника. Такие преобразования позволяют решить две главные проблемы защиты данных: проблему обеспечения *конфиденциальности* (путем лишения противника возможности извлечь информацию из канала связи) и проблему *целостности* (путем лишения противника возможности изменить сообщение так, чтобы изменился его смысл, или ввести ложную информацию в канал связи).

Обобщенная схема криптографической системы, обеспечивающей шифрование передаваемой информации, изображена на следующем рисунке:



Отправитель генерирует *открытый текст* исходного сообщения *M*, которое должно быть передано законному получателю по незащищенному каналу. За каналом следит перехватчик с целью перехватить и раскрыть передаваемое сообщение. Для того, чтобы перехватчик не смог узнать содержание сообщения *M*, отправитель шифрует его с помощью обратимого преобразования E_k и получает *шифротекст* $C=E_k(M)$, который отправляет получателю.

Законный получатель приняв шифротекст *C*, расшифровывает его с помощью обратного преобразования $D_k = E_{k^{-1}}(C)$ и получает исходное сообщение в виде открытого текста *M*.

Преобразование E_k называется *криптоалгоритмом*.

Под *криптографическим ключом K* понимается конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма. Данный ключ, либо его часть, является закрытой информацией, которая должна быть известна только законным участникам криптографического обмена. Утеря секретной части ключа ведет к раскрытию всего защищенного обмена.

Криптоанализ

Любая попытка со стороны перехватчика расшифровать шифротекст *C* для получения открытого текста *M* или зашифровать свой собственный текст *M`* для получения правдоподобного шифротекста *C`*, не имея подлинного ключа, называется *криптоаналитической атакой*.

Если предпринятые криптоаналитические атаки не достигают поставленной цели и криптоаналитик не может, не имея подлинного ключа, вывести *M* из *C* или *C`* из *M`*, то систему называют *криптостойкой*.

Криптоанализ – это наука о раскрытии исходного текста зашифрованного сообщения без доступа к ключу. Успешный криптоанализ может раскрыть исходный текст или ключ.

Традиционные симметричные алгоритмы шифрования

Среди наиболее распространенных простейших алгоритмов шифрования информации можно выделить шифры перестановок и шифры замены (подстановки).

Шифрование перестановкой заключается в том, что символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста.

Примерами шифров перестановки являются шифр «скитала», шифрующие таблицы.

Шифрование заменой (подстановкой) заключается в том, что символы шифруемого текста заменяются символами того же или другого алфавита в соответствие с заранее обусловленной схемой замены.

Примерами шифров замены являются моноалфавитная замена, многоалфавитная замена, шифр Цезаря, шифр Гросфельда, шифр Вижинера.

Система шифрования Цезаря

Шифр Цезаря является частным случаем шифра простой замены. Свое название этот шифр получил по имени римского императора Гая Юлия Цезаря, который использовал этот шифр при переписке с Цицероном (около 50 г. до н.э.).

При шифровании исходного текста методом Цезаря, каждая буква открытого текста заменяется на букву того же алфавита по следующему правилу. Заменяющая буква определяется путем смещения по алфавиту от исходной буквы на K букв (позиций). При достижении конца алфавита выполняется циклический переход к его началу. Смещение K в данном случае определяет ключ шифрования. Совокупность возможных подстановок для больших букв английского алфавита и K=3 представлена в таблице 1.

Таблица 1. Таблица подстановок

A	→	D		H	→	K		O	→	R		V	→	Y
B	→	E		I	→	L		P	→	S		W	→	Z
C	→	F		J	→	M		Q	→	T		X	→	A
D	→	G		K	→	N		R	→	U		Y	→	B
E	→	H		L	→	O		S	→	V		Z	→	C
F	→	I		M	→	P		T	→	W				
G	→	J		N	→	Q		U	→	X				

Математическая модель шифра Цезаря записывается в виде (1)

$$C=(P+K) \bmod M \quad (1)$$

где C – код символа шифротекста, P – код символа открытого текста, K – коэффициент сдвига, M – размер алфавита, mod – операция нахождения остатка от деления на M.

Например, результатом шифрования открытого текста RED APPLE по методу Цезаря с ключом *K*=3 будет являться последовательность UHG ASSOH.

Порядок выполнения лабораторной работы

1. Познакомиться с моделями традиционных симметричных алгоритмов шифрования.
2. Из таблицы 4 взять алгоритм шифрования и его ключ, соответствующие Вашему варианту. Реализовать программный модуль шифрования и дешифрования файлов на жестком диске ПК в соответствии с данным алгоритмом шифрования и ключом.

Контрольные вопросы

1. Охарактеризуйте направление «криптография». Что называют криптографическим ключом?
2. Проклассифицируйте традиционные алгоритмы шифрования. Кратко охарактеризуйте эти классы.
3. Охарактеризуйте методы шифрования Цезаря, простую моноалфавитную замену, G-контурную многоалфавитную замену, простую перестановку, перестановки Гамильтона.
4. Что понимается под криптоанализом?

Таблица 4. Варианты

Вариант	Алгоритм шифрования	Ключ
1	Шифр Цезаря	K=4
2	Простая моноалфавитная замена	a=3, K=2
3	G-контурная многоалфавитная замена	K=33922
4	Простая перестановка	K=632514
5	Перестановки Гамильтона	K=13
6	Шифр Цезаря	K=2
7	Простая моноалфавитная замена	a=7, K=3
8	G-контурная многоалфавитная замена	K=12578
9	Простая перестановка	K=4172536
10	Перестановки Гамильтона	K=32
11	Шифр Цезаря	K=7
12	Простая моноалфавитная замена	a=11, K=2
13	G-контурная многоалфавитная замена	K=13243
14	Простая перестановка	K=32541
15	Перестановки Гамильтона	K=45
16	Шифр Цезаря	K=9
17	Простая моноалфавитная замена	a=13, K=5
18	G-контурная многоалфавитная замена	K=94827
19	Простая перестановка	K=813926457
20	Перестановки Гамильтона	K=14
21	Шифр Цезаря	K=8
22	Простая моноалфавитная замена	a=17, K=4
23	G-контурная многоалфавитная замена	K=37984
24	Простая перестановка	K=3124
25	Перестановки Гамильтона	K=35
26	Шифр Цезаря	K=11
27	Простая моноалфавитная замена	a=19, K=3
28	G-контурная многоалфавитная замена	K=2893475
29	Простая перестановка	K=35124
30	Перестановки Гамильтона	K=53

Лабораторная работа №5

Защита сетей с применением межсетевых экранов

Настройка брандмауэра в Windows

Рекомендуемое оборудование: два компьютера, подключенных напрямую или по сети. ОС Windows , установленная на обоих компьютерах

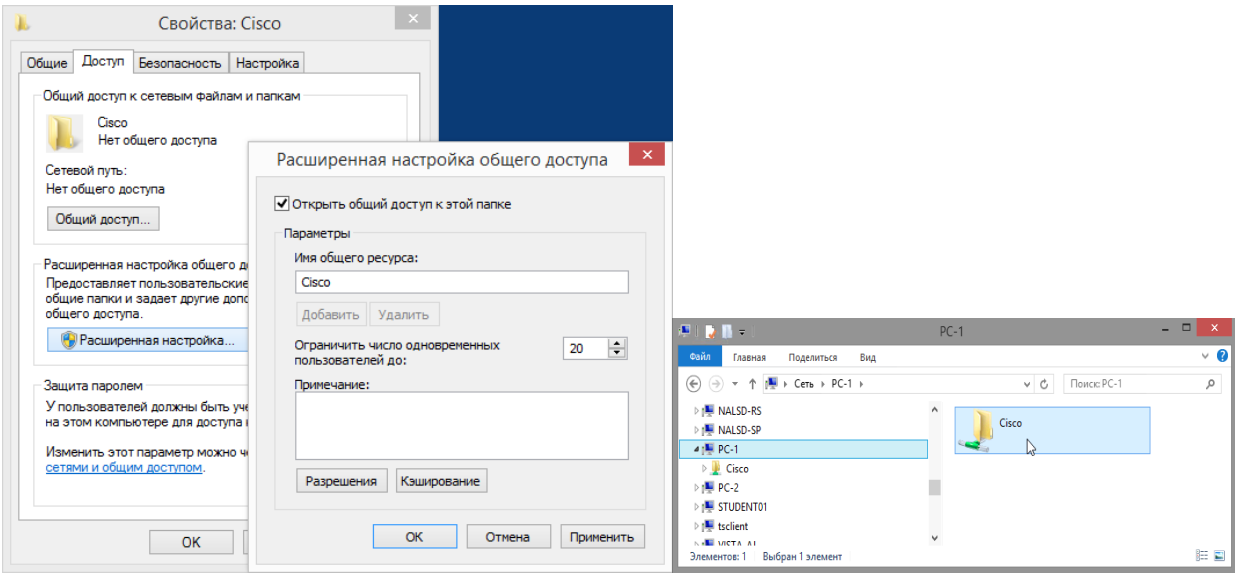
Компьютеры должны находиться в одной рабочей группе и в одной подсети

Создание папки на ПК-1 и предоставление общего доступа к ней

Начните сеанс на ПК-1 под учетной записью участника группы администраторов. Имя пользователя и пароль узнайте у инструктора.

На ПК-1 щелкните область рабочего стола правой кнопкой мыши, затем выберите Создать > Папка. Назовите новую папку Cisco.

Щелкните папку Cisco правой кнопкой мыши и выберите Свойства > Общий доступ > Расширенная настройка общего доступа. Откроется окно Расширенная настройка общего доступа. Щелкните Общий доступ к папке и используйте имя папки по умолчанию — Cisco. Нажмите ОК. Закройте окно свойств папки Cisco.

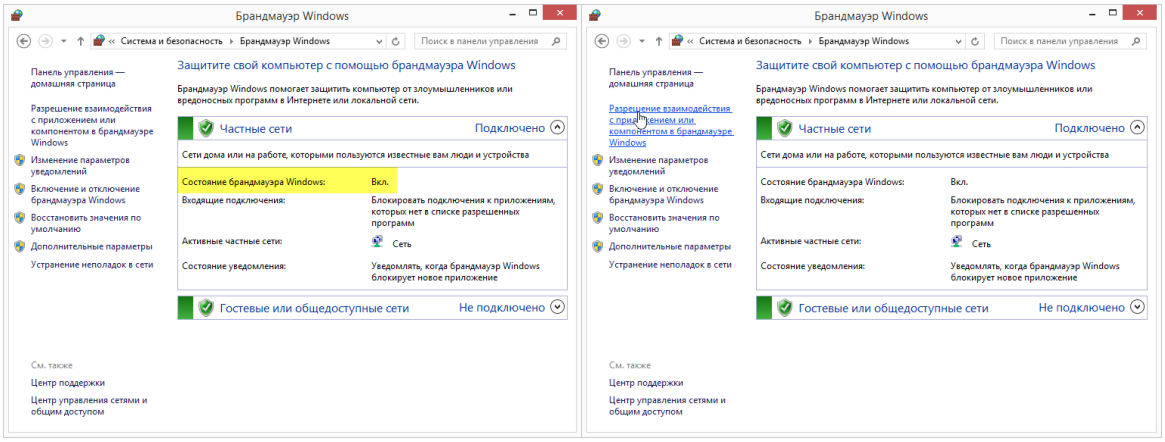


Использование проводника для просмотра общей папки на ПК-1

Начните сеанс на ПК-2 под учетной записью участника группы администраторов. Имя пользователя и пароль узнайте у инструктора.

Откройте Проводник. На панели слева разверните пункт ПК-1 в разделе Сеть.

Чтобы открыть брандмауэр Windows, щелкните Панель управления > Брандмауэр Windows. Брандмауэр Windows по умолчанию включен.

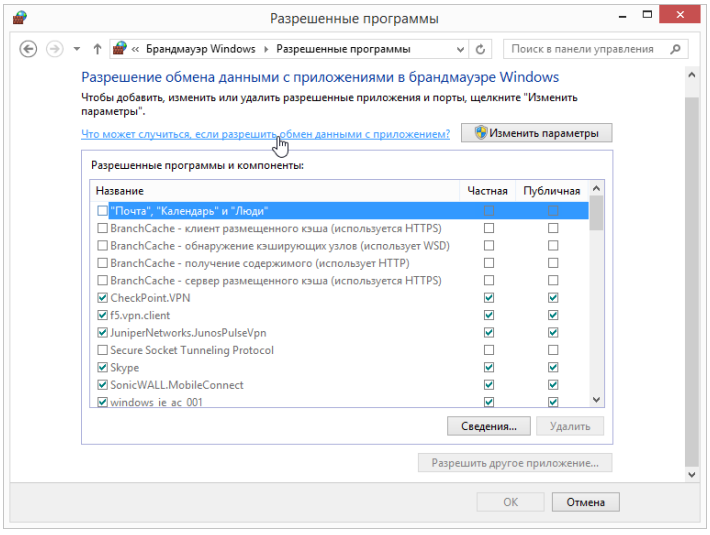


Знакомство со списком разрешенных программ брандмауэра Windows

Щелкните «Разрешение взаимодействия с приложением или компонентом в брандмауэре Windows».

Откроется окно «Разрешенные программы». Программы и службы, которые не блокируются брандмауэром Windows, отмечены флажком.

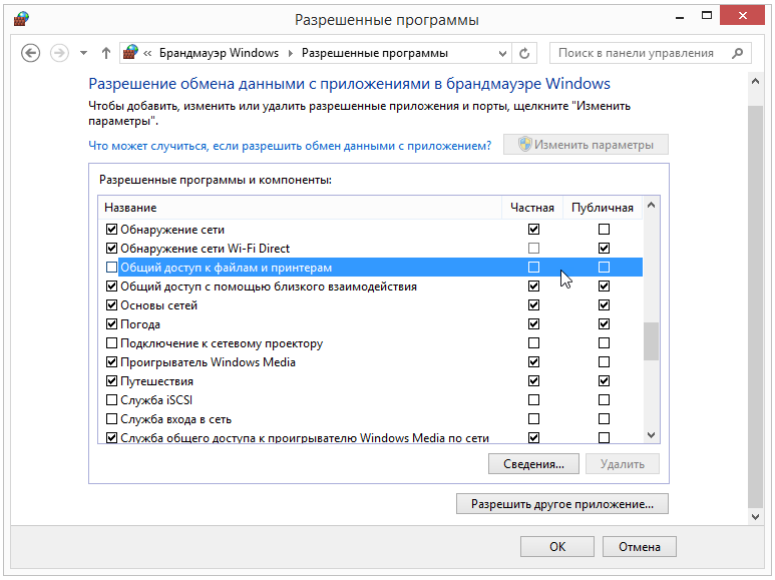
В этот список можно добавлять приложения. Это может быть необходимо, если у вас имеется приложение, требующее связи с внешней сетью, но по какой-то причине брандмауэр Windows не может выполнить настройку автоматически.



Создание большого числа исключений в файле программ и служб может привести к негативным последствиям.

Настройка списка разрешенных программ брандмауэра Windows

Щелкните окно «Разрешенные программы», чтобы активировать его. Щелкните «Изменить параметры». Снимите флажок Общий доступ к файлам и принтерам. Нажмите ОК.



Используя проводник на ПК-2, попробуйте выполнить подключение к ПК-1.

Удалось ли подключиться к ПК-1 и просмотреть общую папку Cisco?

Отобразилось ли на экране ПК-2 сообщение об ошибке? Если да, то что в нем говорится?

Закройте все открытые окна на ПК-2.

На ПК-1 установите флажок Общий доступ к файлам и принтерам. Нажмите ОК.

Снятие и установка флажка должны выполняться без помощи кнопки Изменить параметры.

На ПК-2 снова откройте проводник и попробуйте подключиться к ПК-1. Удалось ли подключиться к компьютеру 1? Почему?

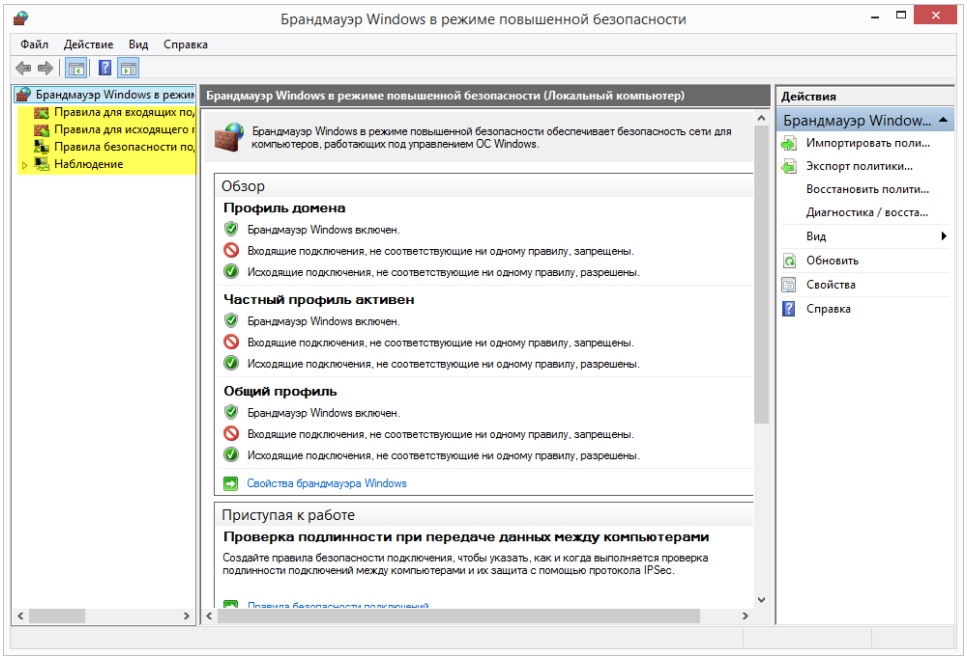
Закройте все открытые окна на ПК-2 и завершите сеанс. Закройте все окна на ПК-1.

Настройка расширенных функций безопасности брандмауэра Windows

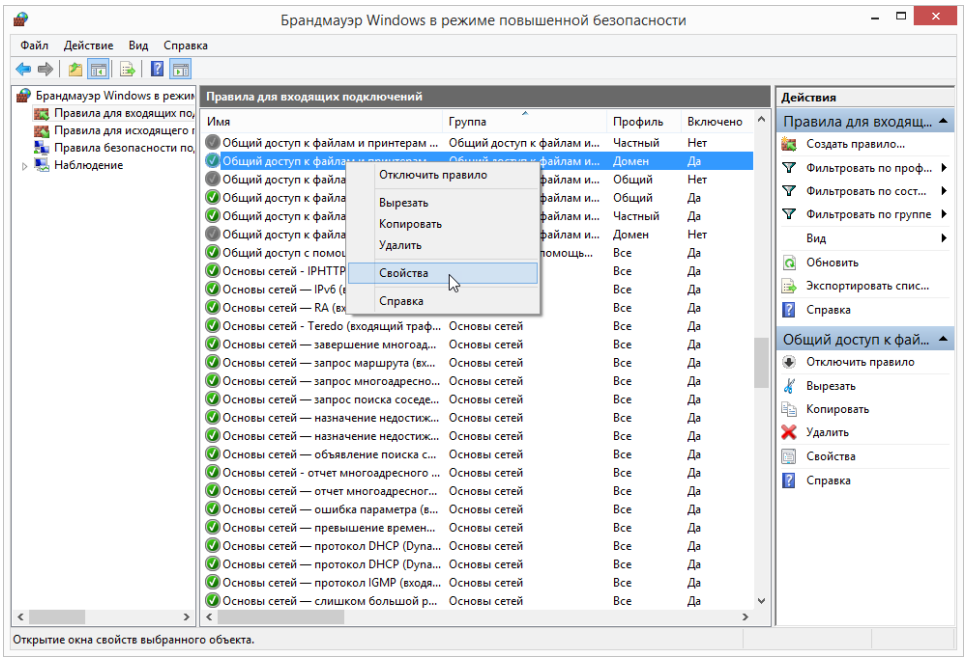
Примечание. Далее на протяжении всей лабораторной работы используется ПК-1.

Щелкните Панель управления > Администрирование > Брандмауэр Windows в режиме повышенной безопасности.

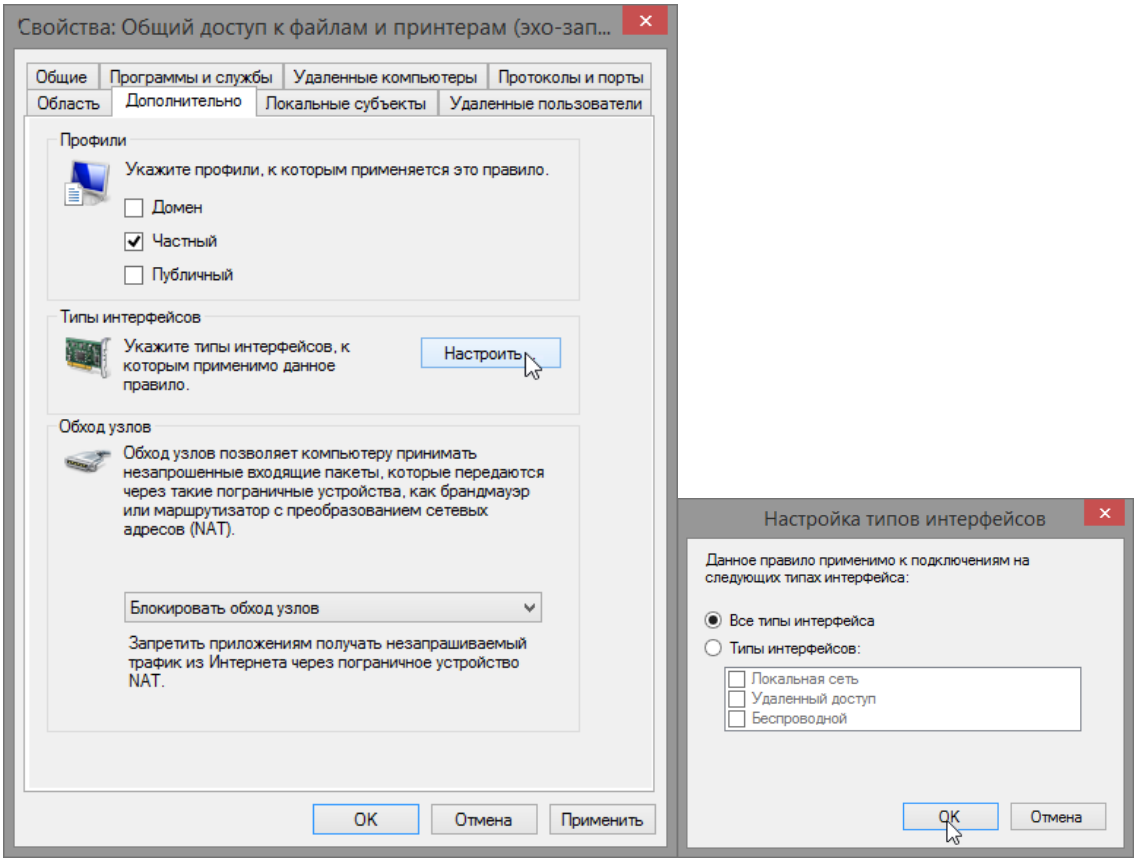
Откроется окно Брандмауэр Windows в режиме повышенной безопасности. На панели слева можно выбрать параметры для настройки: Правила для входящего подключения, Правила для исходящего подключения или Правила безопасности подключения. Чтобы просмотреть состояние настроенных правил, щелкните Мониторинг. Щелкните «Правила для входящего подключения».



Прокрутите панель в центре до правила Общий доступ к файлам и принтерам. Щелкните правило правой кнопкой мыши и выберите «Свойства» и вкладку «Дополнительно».

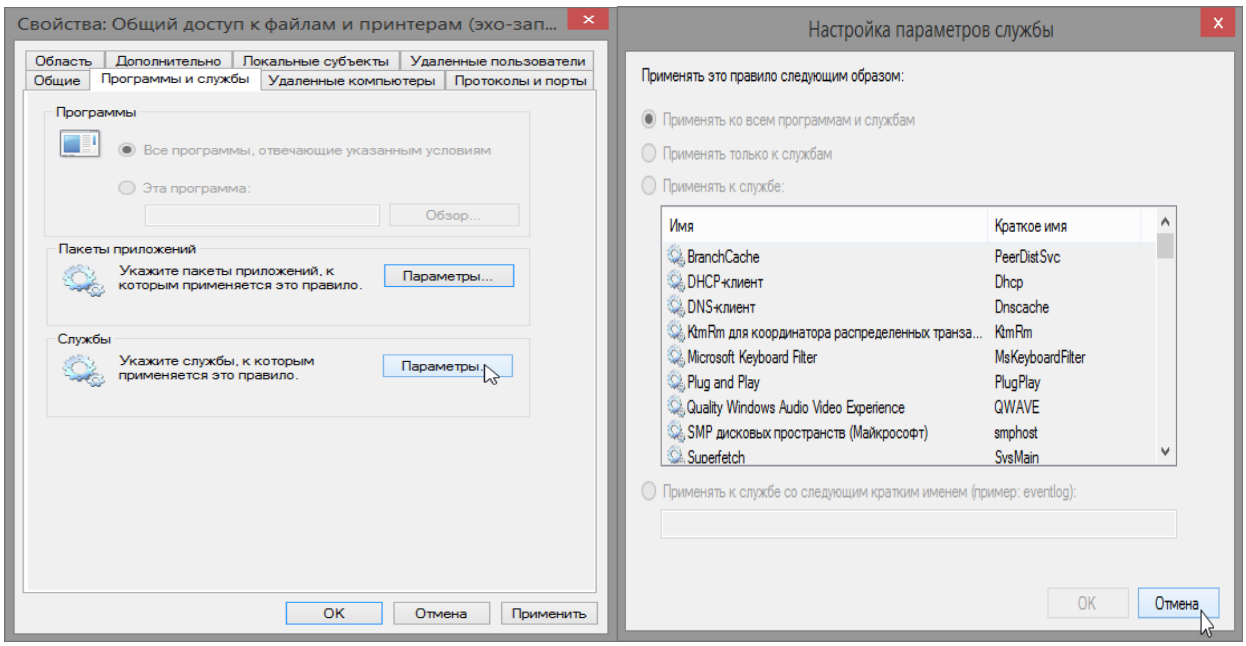


На вкладке «Дополнительно» отображаются профили, используемые компьютером. Щелкните «Настроить» в разделе «Типы интерфейсов».



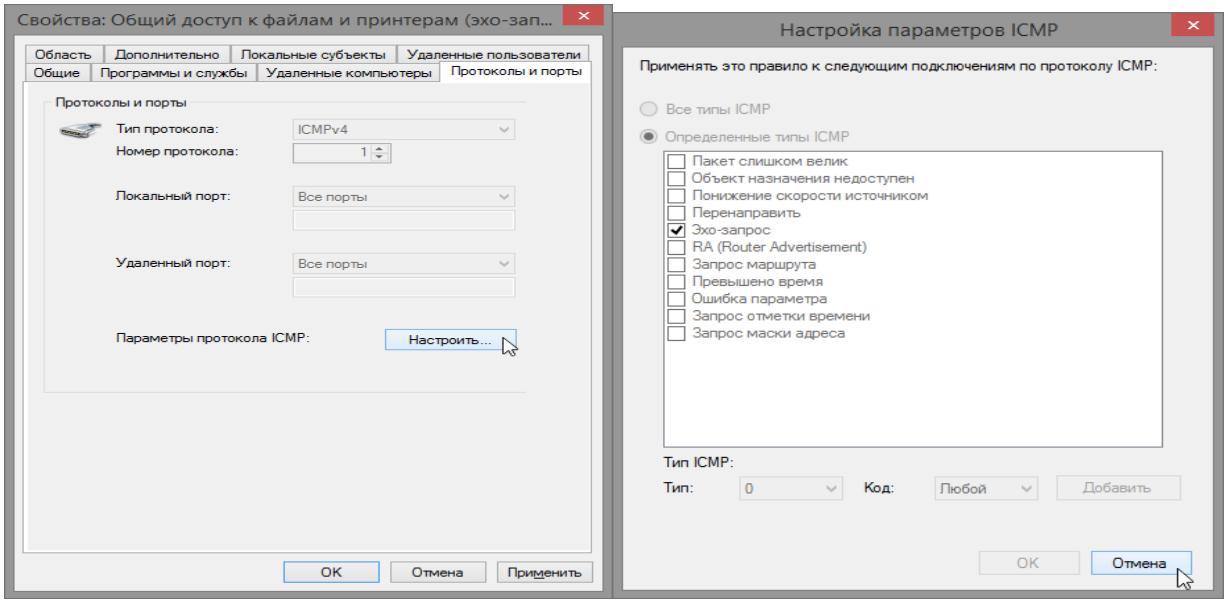
Откроется окно «Настройка типов интерфейсов». Здесь отображаются подключения, настроенные для компьютера. Оставьте флажок «Все типы интерфейсов» и нажмите OK.

Щелкните вкладку «Программы и службы». В разделе «Службы» щелкните «Параметры».



Откроется окно «Настройка параметров службы».

Нажмите «Отмена», чтобы закрыть окно «Настройка параметров служб». Щелкните вкладку «Протоколы и порты».



В разделе параметров протокола ICMP нажмите кнопку Настройка.

Откроется окно Настройка параметров ICMP. При разрешении эхо-запросов пользователи в сети смогут отправлять эхо-запросы на компьютер для определения его присутствия в сети. Закройте все открытые окна на ПК-1.

Основная литература:

1. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е. К. Баранова, А. В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2020. — 320 с. — (Высшее образование). - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1052206 . – Режим доступа: по подписке.

2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. - 2 -е изд., стер. - М.: ИЦ "Академи", 2016. - 256 с.

3. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — М. : ИД «ФОРУМ» : ИНФРА-М, 2017. — 592 с. — Режим доступа: http://znanium.com/bookread2.php?book=546679

Дополнительная литература:

4. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем : учебное пособие / Е. В. Глинская, Н. В. Чичварин. - Москва : ИНФРА-М, 2021. - 118 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016536-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178153 – Режим доступа: по подписке.

5.Электронный документооборот и обеспечение безопасности стандартными средствами windows : учебное пособие / Л.М. Евдокимова, В.В. Корябкин, А.Н. Пылькин, О.Г. Швечкова. – М. : КУРС, 2017. – 296 с. — Режим доступа: http://znanium.com/bookread2.php?book=851088