МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛ-ХОРАЗМИЙ

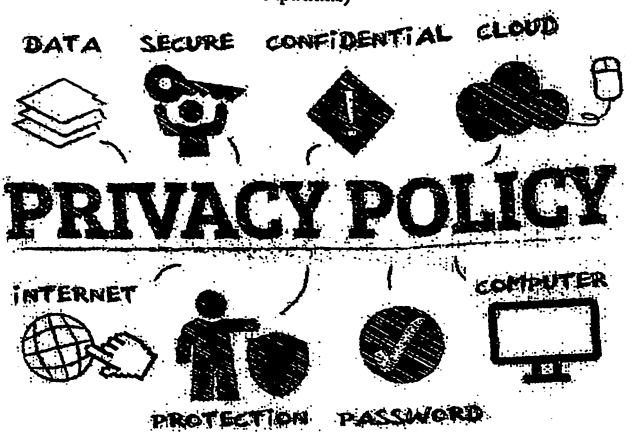
Кафедра «Кибербезопасность и криминалистика»

МЕТОДИЧЕСКОЕ ПОСОБИЕ

по выполнению практических работ по дисциплине

"ПОЛИТИКА КИБЕРБЕЗОПАСНОСТИ"

для студентов бакалавриатуры 5330300- "Информационная безопасность (по отраслям)"



Ташкент – 2022

Это методическое пособие создано для студентов 4 курсов бакалавриатуры по направлению 5330300- "Информационная безопасность (по отраслям)", чтобы приобрести практические навыки по созданию согласованной политики кибербезопасности в организации.

В методической пособии рассматриваются основные вопросы связанные со средствами обеспечения безопасности и их влияние на политику кибербезопасности, вопросы направленные на формирование практических знаний, умений и навыков по правильному формированию политики кибербезопасности межсетевых экранов и антивирусных программ, политик учётных записей и паролей, организация правильной работы в Интернете, а также на развитие самостоятельного мышления обучающихся, умения сопоставлять, анализировать вопросы реагирования и управления инцидентами информационной безопасности. Кроме того, в нем приведены примеры политик безопасности для сред с низким, средним и высоким уровнем угроз.

Составители:

Зокиров О.Ё — и.о. доцент кафедры «Кибербезопасность и криминалистика», ТУИТ

Муминова С.Ш. — старший преподаватель кафедры «Кибербезопасность и криминалистика», ТУИТ

Юлдашева Н.С — ассистент кафедры «Кибербезопасность и криминалистика», ТУИТ

Рецензенты:

Н.Б.Насруллаев — Директор Нурафшанского филиала ТУИТ имени Мухаммад ал-Хоразмий, Phd, доцент

Ш.Р.Гуломов — заведующий кафедрой «Инфомационная безопасность», ТУИТ имени Мухаммад ал-Хоразмий, Phd, доцент

ВВЕДЕНИЕ

В методическом пособии представлены вопросы ввиде практических работ для приобретения и освоения практических навыков по формированию политики безопасности межсетевого экрана, политики безопасности антивирусов и по работе средств защиты от компьютерных вирусов и антивирусных программ, по формированию политики аутентификации пользователей в сети и по защите учетных записей пользователей с помощью Google Authenticator, по изучению политики паролей, по использованию пользователями инструменты управления паролями и по настройке менеджера паролей, по настройке резервного копирования пользовательских данных с помощью облачных сервисов, по изучению средств обеспечения конфиденциальности пользовательских данных в сети интернет, а также, по изучению мер по защите от угроз социальной инженерии (ограничение спама в почте, контроль ссылок).

Курс «Политика кибербезопасности» является предметом по специальности и преподается на 4 курсе обучения. Изучение данного курса требует знания и навыки по дисциплинам связанных с защитой информации, таких как «Основы кибербезопасности», «Безопасность сетей», «Киберправо и киберэтика» и «Безопасность баз данных».

Каждая практическая работа состоит из таких компонентов, как тема практической работы, цель работы, теоретическая и практическая часть, задание и контрольные вопросы. В течение академического семестра студенты должны выполнять задания и предоставлять отчеты на основе практических инструкций. Каждый отчет, независимо от темы практической работы, должен состоят из следующих компонентов:

1. Титульный лист
2. Тема и цель работы.
3. Основная часть (порядок выполнения задания).
4. Ответы на контрольные вопросы
5. Литература

ПРАКТИЧЕСКАЯ РАБОТА №1.
ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ОТ КИБЕРАТАК С ПОМОЩЬЮ МЕЖСЕТЕВОГО ЭКРАНА.

Цель работы: Получить практические навыки по формированию политики безопасности межсетевого экрана и Освоение навыков по установке и настройке межсетевого экрана для защиты данных от атак по локальным и глобальным сетям.

Теоретическая часть.

Политика безопасности межсетевых экранов. Основы и цель. Многие организации присоединили или хотят присоединить свои локальные сети к Интернету, чтобы их пользователи имели легкий доступ к сервисам Интернета. Так как Интернет в целом не является безопасным, машины в этих ЛВС уязвимы к неавторизованному использованию и внешним атакам. Межсетевой экран - это средство защиты, которое можно использовать для управления доступом между надежной сетью и менее надежной. Межсетевой экран - это не одна компонента, а стратегия защиты ресурсов организации, доступных из Интернета. Межсетевой экран выполняет роль стражи между небезопасным Интернетом и более надежными внутренними сетями.

Основная функция межсетевого экрана - централизация управления доступом. Если удаленные пользователи могут получить доступ к внутренним сетям в обход межсетевого экрана, его эффективность близка к нулю. Например, если менеджер, находящийся в командировке, имеет модем, присоединенный к его ПЭВМ в офисе, то он может дозвониться до своего компьютера из командировки, а так как эта ПЭВМ также находится во внутренней защищенной сети, то атакующий, имеющий возможность установить коммутируемое соединение с этой ПЭВМ, может обойти защиту межсетевого экрана. Если пользователь имеет подключение к Интернету у какого-нибудь провайдера Интернета, и часто соединяется с Интернетом со

своей рабочей машины с помощью модема, то он или она устанавливают небезопасное соединение с Интернетом, в обход защиты межсетевого экрана.

Межсетевые экраны часто могут быть использованы для защиты сегментов интранета организации, но этот документ в основном будет описывать проблемы, связанные с Интернетом.

Межсетевые экраны обеспечивают несколько типов защиты:

- они могут блокировать нежелательный трафик;
- они могут направлять входной трафик только к надежным внутренним системам;
- они могут скрыть уязвимые системы, которые нельзя обезопасить от атак из Интернета другим способом;
- они могут протоколировать трафик в и из внутренней сети;
- они могут скрывать информацию, такую как имена систем, топологию сети, типы сетевых устройств и внутренние идентификаторы пользователей, от Интернета;
- они могут обеспечить более надежную аутентификацию, чем та, которую представляют стандартные приложения;

Каждая из этих функций будет описана далее.

Как и для любого средства защиты, нужны определенные компромиссы между удобством работы и безопасностью. Прозрачность - это видимость межсетевого экрана как внутренним пользователям, так и внешним, осуществляющим взаимодействие через межсетевой экран. Межсетевой экран прозрачен для пользователей, если он не мешает им получить доступ к сети. Обычно межсетевые экраны конфигурируются так, чтобы быть прозрачными для внутренних пользователей сети (посылающим пакеты наружу за межсетевой экран); и с другой стороны межсетевой экран конфигурируется так, чтобы быть непрозрачным для внешних пользователей, пытающихся получить доступ к внутренней сети извне. Это

обычно обеспечивает высокий уровень безопасности и не мешает внутренним пользователям.

Примеры политик. Все организации должны использовать как минимум политику для уровня с низким риском. Для среднего риска надо добавить части с пометкой "Средний риск", а для высокого - части с пометкой "Высокий риск" и "Средний риск".

Низкий риск.

Пользователь. Все пользователи, которым требуется доступ к Интернету, должны делать это, используя одобренное организацией программное обеспечение и через Интернет-шлюзы организации.

Между нашими частными сетями и Интернетом установлен межсетевой экран для защиты наших компьютеров. Сотрудники не должны пытаться обойти его при соединении с Интернетом с помощью модемов или программ для сетевого тунеллирования.

Некоторые протоколы были блокированы или их использование ограничено. Если вам требуется для выполнения ваших обязанностей какой-то протокол, вы должны обратиться к начальнику вашего отдела и ответственному за безопасное использование Интернета.

Начальник отдела. Должен быть помещен межсетевой экран между сетью компании и Интернетом для того, чтобы предотвратить доступ к сети компании из ненадежных сетей. Межсетевой экран должен быть выбран ответственным за сетевые сервисы, он же отвечает за его сопровождение.

Все остальные формы доступа к Интернету (такие как модемы) из сети организации, или сетей, подключенных к сети организации, должны быть запрещены.

Все пользователи, которым требуется доступ к Интернету, должны делать это с помощью одобренных организацией программ и через шлюзы с Интернетом.

Сотрудник отдела автоматизации. Все Межсетевые экраны при аварийном завершении должны делать невозможным доступ ни к каким

сервисам, и требовать прибытия администратора Межсетевого экрана для восстановления доступа к Интернету.

Маршрутизация источника должна быть запрещена на всех Межсетевого экранах и внешних маршрутизаторах.

Межсетевой экран должен отвергать трафик из внешних интерфейсов, который имеет такой вид, будто он прибыл из внутренней сети.

Межсетевой экран должен вести детальные системные журналы всех сеансов, чтобы их можно было просмотреть на предмет выявления нештатных ситуаций в работе.

Для хранения журналов должен использоваться такой носитель и место хранения, чтобы доступ к ним ограничивался только доверенным персоналом.

Межсетевые экраны должны тестироваться перед началом работы и проверяться на предмет правильности конфигурации.

Межсетевой экран должен быть сконфигурирован так, чтобы он был прозрачен для выходящих соединений. Все входящие соединения должны перехватываться и пропускаться через межсетевой экран, если только противное решение явно непринято ответственным за сетевые сервисы.

Должна постоянно вестись подробная документация на межсетевой экран и храниться в безопасном месте. Такая документация должна включать как минимум схему сети организации с IP-адресами всех сетевых устройств, IP-адреса машин у провайдера Интернета, таких как внешние сервера новостей, маршрутизаторы, DNS-сервера и т.д., и другие параметры конфигурации, такие как правила фильтрации пакетов и т.д. Такая документация должна обновляться при изменении конфигурации Межсетевого экрана.

Средний риск.

Пользователь. Для удаленного доступа к внутренним системам организации требуется усиленная аутентификация с помощью одноразовых паролей и смарт-карт.

Начальник отдела. Администраторы Межсетевого экрана и другие руководители, ответственные за компьютерную безопасность, должны регулярно пересматривать политику сетевой безопасности (не реже чем раз в три месяца). При изменении требований к работе в сети и сетевым сервисам политика безопасности должна быть обновлена и утверждена заново. При необходимости внесения изменений администратора Межсетевого экрана отвечает за реализацию изменений на межсетевом экране и модификацию политики.

Структура и параметры внутренней сети организации не должны быть видимы из-за Межсетевого экрана.

Сотрудник отдела автоматизации. Межсетевой экран должен быть сконфигурирован так, чтобы по умолчанию все сервисы, которые не разрешены, были запрещены. Должен производиться регулярный аудит его журналов на предмет выявления попыток проникновения или неверного использования Интернета.

Межсетевой экран должен практически сразу уведомлять системного администратора при возникновении ситуации, требующей его немедленного вмешательства, такой как проникновение в сеть, отсутствие места на диске и т.д.

Межсетевой экран должен работать на специальном компьютере - все программы, не относящиеся к межсетевому экрану, такие как компиляторы, редакторы, коммуникационные программы и т.д., должны быть удалены или доступ к ним должен быть заблокирован.

Высокий риск.

Пользователь. Использование Интернета в личных целях с систем организации запрещено. Весь доступ к Интернету протоколируется. Сотрудники, нарушающие данную политику, будут наказаны.

Ваш браузер был сконфигурирован так, что доступ к ряду сайтов запрещен. О всех попытках получить доступ к этим сайтам будет доложено вашему начальнику.

Начальник отдела. Использование Интернета в личных целях с систем организации запрещено. Весь доступ к Интернету протоколируется. Сотрудники, нарушающие данную политику, будут наказаны.

Сотрудник отдела автоматизации. Весь доступ к Интернету должен протоколироваться.

Практическая часть.

Более чем очевидно, что конечные пользователи за все время, проводимое за компьютерами, работают с тем или иным программным обеспечением. В наше время чуть ли не каждый продукт в той или иной степени связан с локальными или глобальными сетями и работает с трафиком. Стандартной практикой в большинстве компаний, которые уделяют должное внимание безопасности, представляет собой процедура блокирования всего неавторизованного трафика для прослушивания портов TCP и UDP.

В случае с клиентскими операционными системами и приложениями, которые принимают входящий трафик, пользователям по умолчанию выводится диалог, информирующий о том, что определенный запрос был заблокирован и пользователю следует предпринять какие-либо меры, а в случае же с серверными операционными системами никакого диалога не будет выводиться. Следовательно, если пользователи работают с какой-то специфической программой, которая должна получать трафик, для нее должно быть создано отдельное правило в межсетевом экране Windows.

Правилами для программы являются практически такие же правила, которые разработчики программного обеспечения самостоятельно генерируют при инсталляции программного продукта. Этот тип правил служит для создания отдельного правила, разрешающего или блокирующего подключения конкретного исполняемого файла, независимо от используемых номеров портов. То есть при его ссздании вы не ограничиваетесь определенными портами, о существовании которых можете и не знать. Именно по этой причине данный тип правила для

большинства людей может оказаться самым полезным и актуальным, так как далеко не каждый пользователь (и иногда администратор) имеет точное представление о том, какие именно порты использует конкретная программа. Лучше всего в большинстве случаев применять именно этот тип правила, но стоит обратить внимание на то, что данный тип не применяется в том случае, если конкретная служба не содержит собственный исполняемый файл.

Давайте посмотрим, как именно создается этот тип правила. Исключительно для примера, все следующие сценарии будут создаваться в оснастке редактора управления групповыми политиками отдельного объекта GPO «**Правила межсетевого экрана**», который будет в тестовых целях связан со всем доменом фиктивной компании. Помимо данной оснастки, естественно, также можно использовать оснастку «**Межсетевой экран Windows в режиме повышенной безопасности**» (**Windows Firewall with Advanced Security**), для вызова которой следует лишь запустить файл **wf.msc**. Итак, для создания такого правила достаточно выполнить следующие действия:

1. В оснастке редактора управления групповыми политиками следует перейти к узлу **Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Межсетевой экран Windows в режиме повышенной безопасности → Межсетевой экран Windows в режиме повышенной безопасности Правила для входящих подключений (Computer Configuration → Policies → Windows Setting → Security Settings → Windows Firewall with Advanced Security → Windows Firewall with Advanced Security Inbound Rules);**
2. В области сведений вызовите контекстное меню и оттуда выберите команду «**Создать правило**» (**New Rule**), как показано на рисунке №1.1.
3. На первой странице отобразившегося мастера создания правила для нового входящего подключения – «**Тип правила**» (**Rule Type**) вам предоставляются возможности выбора типа создаваемого правила. Так как

изначально запланировано создать правило для программы, можно не выполнять каких-либо действий, а просто оставить переключатель на опции «Для программы» (Program) и нажать на кнопку «Далее» (Next), как видно на рисунке №1.2.

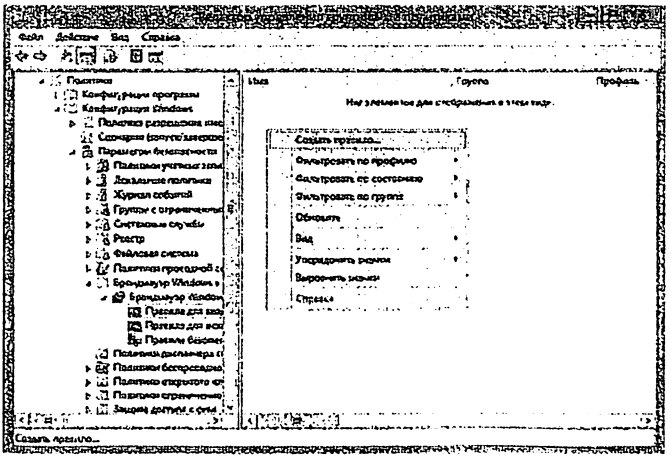


Рис. 1.1. Начало создания правила для входящих подключений

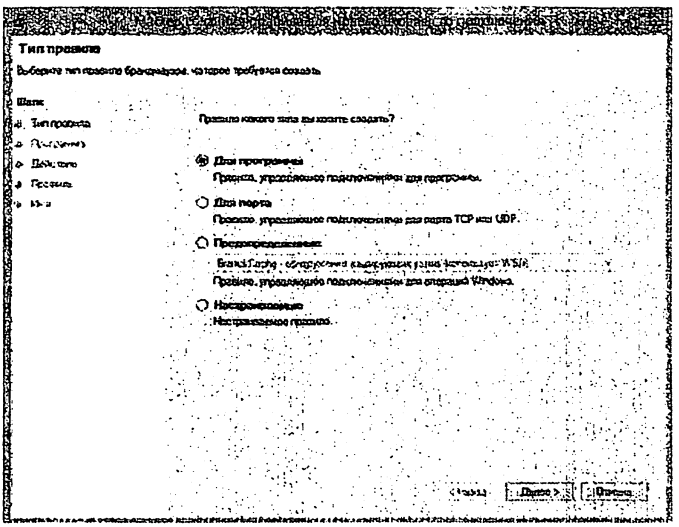


Рис. 1.2. Выбор типа создаваемого правила для входящих подключений

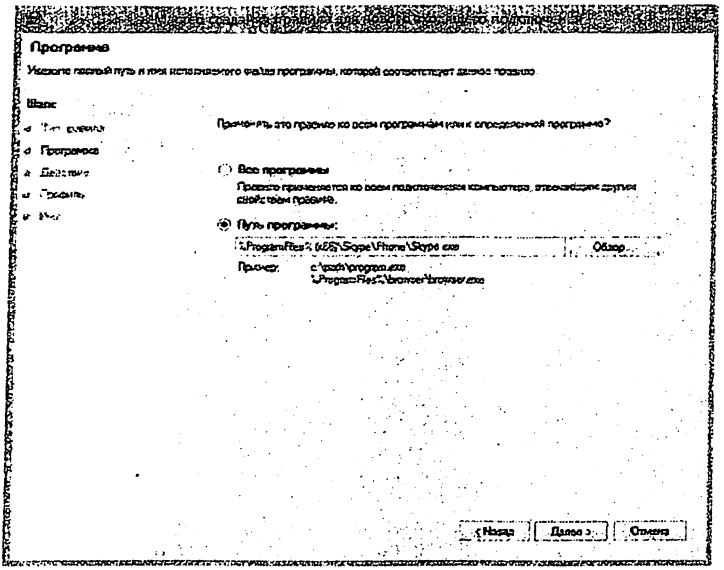


Рис. 1.3. Добавление пути к установленному программному продукту

4. Попав на страницу **«Программа» (Program)**, вам следует указать путь к исполняемому файлу, для которого создается само правило. Например, в данном случае запретим все входящие подключения для программы **«Skype»**, то есть в текстовом поле **«Путь программы» (This program path)** будет указано **«C:Program Files (x86)SkypePhoneSkype.exe»** (естественно, если у вас проинсталлированы 64-разрядные операционные системы не у всех пользователей и нужно указать путь к программе, расположенной в традиционной папке **%Program Files%**, нужно будет создать идентичное правило, но с другим путем). Данную страницу мастера видно на рисунке №1.3.

5. Теперь на следующей странице мастера, которая называется **«Действие» (Action)**, следует указать требуемое действие для создаваемого вами правила. На данной странице вы можете найти три основных действия для межсетевого экрана Windows, а именно:

- **Разрешить подключение (Allow the Connection).** При выборе данного действия вы разрешаете все подключения, которые соответствуют критериям, указанным на всех предыдущих страницах мастера;
- **Разрешить безопасное подключение (Allow the connection if it is secure).** Это значение для правила межсетевого экрана Windows в режиме повышенной безопасности позволяет разрешать подключения только в том случае, если они соответствуют критериям, которые были указаны вами ранее, а также защищены по протоколу IPSec;
- **Блокировать подключение (Block the connection).** В этом случае межсетевой экран Windows в режиме повышенной безопасности будет сбрасывать любые попытки подключения, которые соответствуют указанным вами ранее критериям. Несмотря на то, что изначально все подключения блокируются межсетевым экраном, данное значение целесообразно выбирать в том случае, если вам нужно запретить подключения для конкретного приложения.

В данном примере исключительно для того, чтобы результат сразу же был заметен, входящий трафик для указанного приложения будет запрещаться, а это означает, что переключатель должен быть установлен на последней опции, то есть «**Блокировать подключение**» (**Block the Connection**).

6. На странице «**Профиль**» (**Profile**) выбирается интересующий в данном случае профиль. В этом примере, будет выбираться профиль «**Доменный**» (**Domain**);

7. На последней странице данного мастера, которая называется «**Имя**» (**Name**), достаточно только указать имя для создаваемого правила. В случае необходимости будет крайне полезно, если вы в соответствующее поле добавите подробное описание своего правила. А само правило будет

названо «**Skype x86 on 64 OS**». По завершению выбора опций для всех страниц мастера следует нажать на кнопку «**Готово**» (**Finish**);

8. Теперь осталось повторить идентичные действия, но для исходящих правил межсетевого экрана Windows.

Осталось проверить полученные результаты. Для дополнительного тестирования может оказать неоценимую помощь сниффер. То есть следует открыть тестируемое приложение и попробовать получить данные. В результате, как вы видите на рисунке №1.4, приложению не удалось подключиться к сети, а также после активации таких правил прекратил передаваться трафик.

Права для порта. Приложениями может все не ограничиться. В том случае, если у вас пользователи могут использовать несколько различных приложений, которые получают трафик по определенному порту, можно не заморачиваться с правилами для каждого приложения, а просто ограничить пользовательский трафик для конкретных портов TCP или UDP и использовать только те порты, которые реально будут востребованы вашими корпоративными приложениями. Такой метод в некоторой степени спасет вас от определенного количества атак извне.

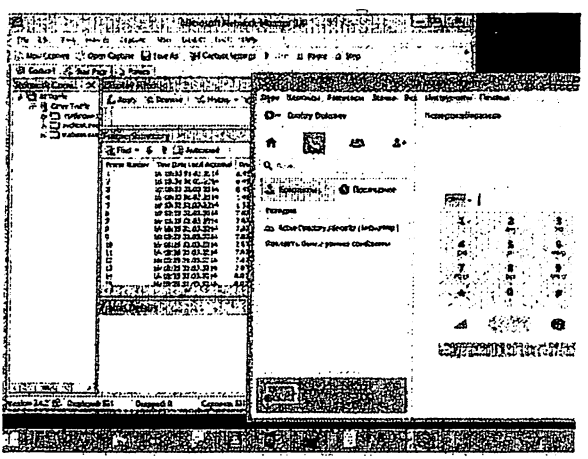


Рис. 1.4. Результат применения правила межсетевого экрана Windows

На этот раз будет продемонстрирован пример блокировки TCP порта 110, который, как вы знаете, отвечает за прием почты, – протокол Post Office Protocol v3, POP3. Выполняются такие действия:

1. В редакторе управления групповыми политиками следует перейти к тому же узлу, что и в предыдущем примере, а затем из контекстного меню области сведений выбрать команду **«Создать правило» (New Rule)**, как было показано выше;

2. На этот раз на странице **«Тип правила» (Rule Type)** вам нужно установить переключатель на опцию **«Для порта» (Port)** и перейти к следующей странице;

3. Как видно на рисунке №1.5, после выбора указанной на предыдущем шаге опции вы перейдете на страницу **«Протокол и порты» (Protocols and Ports)**, где вам нужно в первом управляющем элементе **«Укажите протокол, к которому будет применяться это правило» (Does the rule apply to TCP or UDP)** выбрать тип протокола (UDP либо TCP), например, **«Протокол TCP» (TCP)**, а в группе параметров, отвечающих за определение портов, нужно установить переключатель на опцию **«Определенные локальные порты» (Specific local ports)** и в соответствующем текстовом поле указать номер порта – **110**;

4. На странице определения действия для правила вам нужно точно так же, как и в предыдущем примере, установить переключатель на опцию **«Блокировать подключение» (Block the Connection)**, а затем переходить к следующей странице мастера;

5. На странице **«Профиль» (Profile)** так же выбирается необходимый профиль, например, доменный. Затем можно двигаться дальше;

6. Последняя страница, страница **«Имя» (Name)**, на которой осталось указать имя для создаваемого правила, например, **«Blocking 110 Port»**, и сохранить новое правило;

7. Как и в предыдущем примере, далее создается идентичное правило для исходящих подключений.

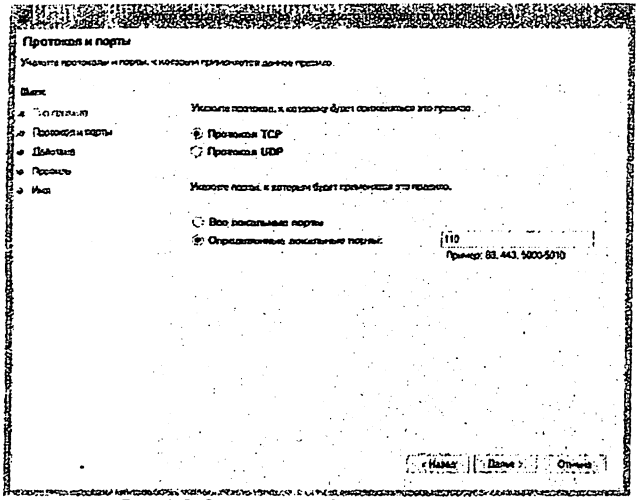


Рис. 1.5. Определение блокируемых портов

Для проверки работы назначенных правил запускаем почтовый клиент и попробуем принять новую почту. Как вы видите на рисунке №1.6, при попытке получения почтовой корреспонденции при помощи POP3 должна вывалиться следующая ошибка:

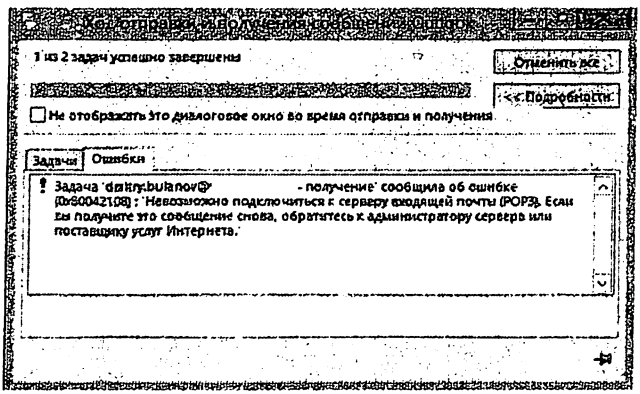


Рис. 1.6. Попытка получения новой почты

Предопределенные правила. Разработчики операционных систем Windows, естественно, знают о различных сценариях, которые могут быть

востребованы системными администраторами в корпоративной среде для реализации той или иной функциональной возможности. Именно по этой причине межсетевой экран Windows в режиме повышенной безопасности включает в себя ряд предопределенных правил, которые можно в любой момент включить для полноценной работы такой функциональной возможности, как, скажем, BranchCache, для общего доступа к проигрывателю Windows Media по сети или через сеть Интернет, для удаленной работы с инструментарием управления Windows, удалённого управления межсетевым экраном, журналом событий, службами, назначенными заданиями или целой операционной системой. Обо всем этом в корпорации Microsoft уже подумали за вас, и для включения той или иной возможности нужно всего лишь, грубо говоря, нажать на несколько кнопок.

Как вы скорее всего помните, такое средство отладки неисправностей, связанных с функциональными возможностями групповой политики, как **«результирующая групповая политика»**, требует, чтобы на клиентском компьютере была запущена и работала служба инструментария управления Windows, то есть WMI. Также будет неплохо, если и во входящих правилах межсетевого экрана Windows будет включена возможность использования инструментария WMI. Как же можно быстро сгенерировать такое правило?

1. В очередной раз в уже открытом требуемом узле редактора управления групповыми политиками следует из контекстного меню области сведений вызвать команду, отвечающую за создание нового правила для входящих подключений межсетевого экрана Windows в режиме повышенной безопасности;

2. На странице выбора типа правила в этом случае следует остановиться на опции **«Предопределенные» (Predefined)**, где из раскрывающегося списка вы можете сразу выбрать требуемый тип правила. Например, как видно в данном примере, нужно остановить свой выбор на правиле **«Инструментарий управления Windows (WMI)» (Windows Management Instrumentation (WMI))**. Между прочим, невозможно не заметить (см. Рис.

№1.7.), что таких предопределенных правил более 40 разновидностей. После выбора требуемого предопределенного правила можно смело нажимать на кнопку «Далее» (Next);

3. На новой странице – странице «Предопред. правила» (Predefined Rules) вы можете выбрать правила, которые операционная система Windows посчитает необходимыми для реализации выбранного вами действия. Например, как видно на рисунке №1.8., чтобы добавить исключения для инструментария управления Windows, вам нужно создать правила для асинхронного входящего трафика, а также для входящего трафика WMI и DCOM. Установив флажки на создаваемых правилах, можно переходить к следующей странице мастера.

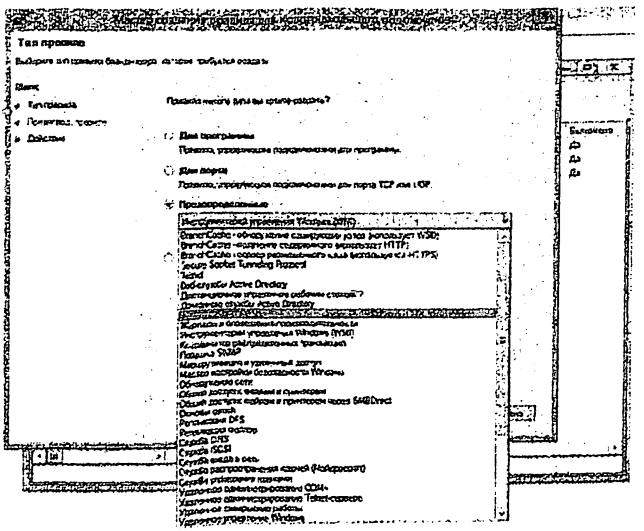


Рис. 1.7. Выбор предопределенного правила межсетевого экрана Windows

4. В случае с предопределенными правилами на последней странице мастера создания правил для входящего подключения вам следует выбрать не имя для создаваемых правил (оно ведь было определено на предыдущей странице мастера), а требуемое действия для всех создаваемых правил. Так как в этом случае нужно разрешить ходить трафику, выбирается действие

«**Разрешить подключение**» (**Allow the Connection**), и после этого сами правила создаются.

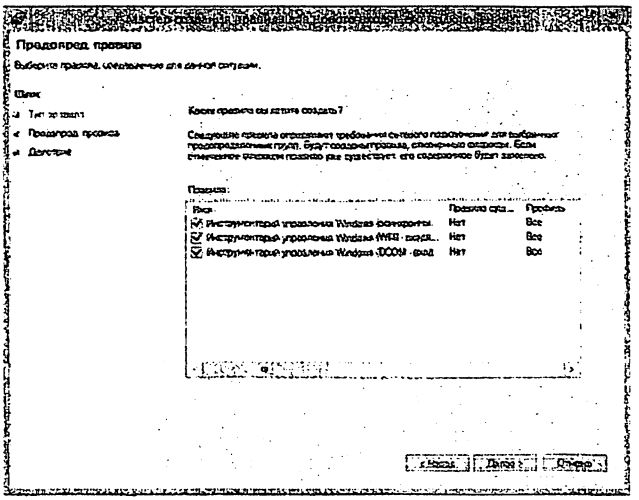


Рис. 1.8. Включение создаваемых правил

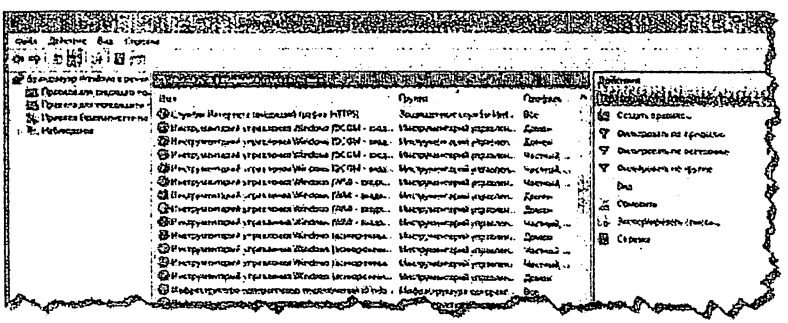


Рис. 1.9. Созданные правила для WMI

Как видно на рисунке №1.9, после обновления параметров групповой политики такие правила успешно создаются, и они будут фигурировать в оснастке «**Межсетевой экран Windows в режиме повышенной безопасности**».

Настраиваемые правила межсетевого экрана Windows. Помимо описанных ранее трех примеров, еще можно выделить несколько

распространенных дополнительных типов создаваемых правил межсетевого экрана Windows, к которым можно отнести:

- Создание правила для конкретной системной службы;
- Создание правила для стороннего протокола;
- Применение правил только для избранных IP-адресов.

Создание правила для системной службы. Чтобы не делать длинного вступления к данному подразделу, просто скажу, что в следующей пошаговой инструкции вы узнаете о том, как можно запретить входящие подключения для службы Telnet. Для этого выполняются следующие действия:

1. Из соответствующего узла редактора управления групповыми политиками вызывается мастер создания правил для нового входящего подключения;
2. На первой странице мастера выбирается тип правила **«Настраиваемые» (Custom)**, после чего можно переходить к следующей странице мастера;
3. Как вы сразу заметите, в этом случае страница **«Программа» (Program)** будет немного отличаться от одноименной страницы первого приведенного выше примера, так как теперь, помимо основного переключателя между всеми установленными на компьютере программами и путем для определенной программы, еще можно найти кнопку, предназначенную для выбора используемой в правиле системной службы. Так как известно, что основная программа, отвечающая за telnet – это **tlntsvr.exe,** переключатель устанавливается на опцию **«Путь программы» (This program path)**, а в текстовом поле вводится **«%systemroot%system32tlntsvr.exe»**. Сразу отмечу, что эта программа может работать не только со службой telnet, поэтому, чтобы ограничить область применения правила в данном случае, придется воспользоваться соответствующей кнопкой для выбора служб, то есть кнопкой **«Настроить» (Customize)** из раздела **«Службы» (Services)**. \

Как видно на рисунке №1.10, по нажатию на эту кнопку перед вами отобразится новое диалоговое окно, при помощи которого вы можете выбрать сразу все возможные программы и службы, только все службы, указать конкретную службу или же выбрать несколько служб на основании указанных вами критериев. Обязательно учтите тот момент, что, как и в случае с остальными компонентами групповой политики, данный список позволяет вам выбирать только те службы, которые проинсталлированы на том компьютере, на котором создается объект групповой политики. Этот момент может оказаться очень важным при планировании и реализации самих объектов GPO. В данном примере устанавливаем переключатель на опцию «**Применять к службе**» (**Apply to this service**) и выбираем службу **Telnet**;

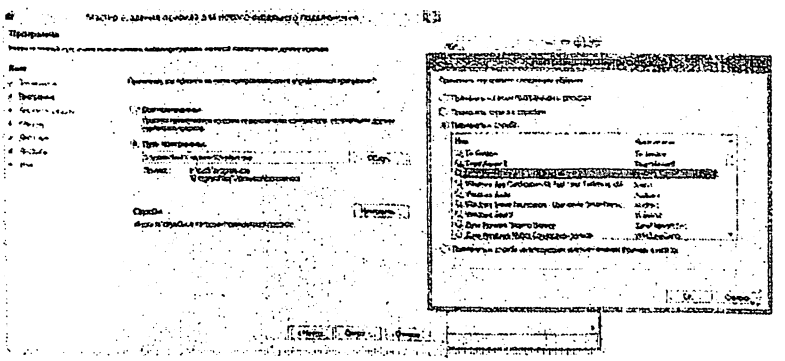


Рис. 1.10. Определение службы Telnet

4. Страница «**Протокол и порты**» (**Protocols and Ports**), по сути, может оставаться без изменений. То есть в качестве типа протокола остается любой протокол, что означает отсутствие возможности настроек локальных и удаленных портов.

5. Очередная страница мастера – совершенно новая страница «**Область**» (**Scope**) – на данном этапе не подлежит изменениям, так как о ней будем говорить подробнее немного ниже. Сейчас же сразу переходим на следующую страницу;

6. На уже знакомой по предыдущим примерам странице «**Действие**» (**Action**) выбирается требуемое действие. Так как в данном примере стоит задача, связанная с блокировкой входящих подключений по Telnet, здесь переключатель устанавливается на опцию «**Блокировать подключение**» (**Block the connection**);

7. Следующей страницей мастера будет страница «**Профиль**» (**Profile**), на которой принято выбирать профили, к которым будет применяться правило. В принципе, в этом примере устанавливаются флажки для всех трех профилей, после чего можно переходить к последней странице мастера;

8. На странице «**Имя**» (**Name**) следует только указать имя создаваемого правила, например, «**Telnet deny**», и сохранить все изменения для нового правила межсетевого экрана Windows.

Настало время проверить, будет ли применяться такое правило должным образом. Для этого открывается окно командной строки и вводится telnet <имя *Telnet* сервера>. Как вы видите на рисунке №1.11, у нас даже не дошло дело до ввода какой-либо простейшей команды вроде **dir**, то есть просмотр каталога. Сразу же при попытке подключения к telnet-серверу командная оболочка Windows PowerShell выдала ошибку, свидетельствующую о невозможности подключения к серверу при помощи 23-го порта.

Рис. 1.11. Ошибка подключения к Telnet-серверу

Создание правила для стороннего протокола. Помимо создания правил для системных служб, вы также можете создавать правила для специфических протоколов и портов. Как вы заметили на одной из первых иллюстраций, при помощи правил для порта вам предоставляется возможность выбрать один или несколько TCP/UDP портов. Но как быть,

если вам нужно сгенерировать новое правило для входящего трафика для какого-либо постороннего протокола, например, ICMP, IGMI или L2TP? Для решения такой задачи, как и в случае с предыдущим примером, вам нужно воспользоваться возможностью создания настраиваемых правил межсетевого экрана Windows.

В следующем примере я продемонстрирую, каким образом можно заблокировать весь ICMP-v4-трафик. Итак:

1. В редакторе управления групповой политикой из контекстного меню области сведений выберите опцию создания нового правила для входящих подключений;

2. На первой странице мастера, как я уже упомянул выше, следует установить переключатель на опцию «**Настраиваемые**» (**Custom**) и перейти ко второй странице мастера;

3. Здесь, на странице «**Программа**» (**Program**), так как согласно условиям поставленной выше задачи должен блокироваться весь входящий трафик для протокола ICMP-v4, достаточно установить переключатель на опции «**Все программы**» (**All Programs**) и нажать на кнопку «**Далее**» (**Next**);

4. После того как вы перейдете на страницу «**Порты**» (**Ports**), вы сможете из первого раскрывающегося списка «**Тип протокола**» (**Protocol Type**) выбрать необходимый тип протокола. Обратите внимание на то, что в Microsoft сразу постарались существенно упростить многим администраторам жизнь, добавив наиболее распространенные, по мнению команды разработчиков межсетевого экрана Windows, протоколы транспортного уровня. К ним можно отнести:

- IPv6 Hop-by-Hop Option, он же **HOPOPT**, зарегистрированный под номером 0;
- Протокол управляющих сообщений, используемый для передачи сообщений об ошибках, Internet Control Message Protocol (**ICMP-v4**) под номером 1, который, собственно, нас интересует в данном случае;

- Протокол управления групповой передачей данных Internet Group Management Protocol – **IGMP** (номер 2);
- Протокол управления передачей **TCP** (номер 6);
- Протокол **UDP** (Протокол пользовательских дейтаграмм, номер 17);
- Протокол инкапсуляции **IPv6** – номер 41;
- Протокол Routing Header for IPv6, который называется **IPv6-Route** и маркируется под номером 43;
- Следующий по порядку протокол – Fragment Header for IPv6 — **IPv6-Frag**, номер 44;
- Протокол туннелирования сетевых пакетов, Generic Routing Encapsulation, **GRE**, номер 47;
- Протокол управляющих сообщений для IPv6, **IPv6-ICMP**, номер 58;
- Протокол под номером 59 – No Next Header for IPv6, **IPv6-NoNxt**;
- Протокол **IPv6-Opts** (Destination Options for IPv6), номер 60;
- Протокол объединения группы маршрутизаторов в один виртуальный маршрутизатор и назначения им общего IP-адреса (**VRRP**) с номером 112;
- Сетевой протокол надёжной многоадресной передачи данных **Pragmatic General Multicast (PGM)**, номер 113;
- А также последний предоставляемый в данном списке туннельный протокол, использующийся для поддержки виртуальных частных сетей, Layer Two Tunneling Protocol Version 3 (**L2TP**), номер 115.

Между прочим, по вполне понятным причинам, локальные и удаленные порты вы можете указывать только в том случае, если из списка выбирается либо протокол TCP, либо UDP.

Естественно, в данном раскрывающемся списке предоставлены далеко не все доступные протоколы (их более 140), и, если вам понадобится указать какой-то уникальный протокол, вы всегда можете из этого списка выбрать опцию **«Настроить»** (**Custom**) и в соответствующем текстовом поле указать номер (не наименование, а именно номер) требуемого

протокола. Например, если вам нужно в правиле межсетевого экрана указать протокол RDP, вы просто вводите число 27.

В данном примере следует из этого списка выбрать протокол ICMP-v4 и, если вы нуждаетесь в дополнительной настройке данного протокола, нажать в нижней части диалогового окна на кнопку «**Настройка**» (**Customize**). В отобразившемся диалоговом окне, как видно на рисунке №1.12, вы можете выбрать определенные типы ICMP, которые будут применяться к вашему правилу. В нашем примере будут использоваться все типы, поэтому изменения вносить в текущем диалоговом окне не обязательно. После того как все изменения на данной странице мастера будут внесены, можно нажимать на кнопку «**Далее**» (**Next**);

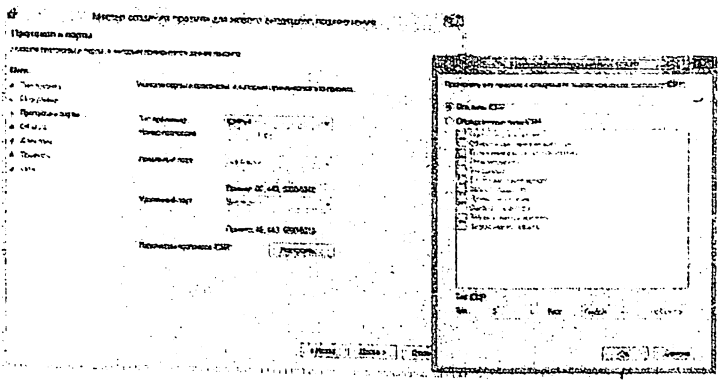


Рис. 1.12. Страница протоколов и портов настраиваемого правила, а также диалоговое окно настройки параметров ICMP

5. Страница «**Область**» (**Scope**) в очередной раз пропускается, а на странице «**Действие**» (**Action**) в соответствии с поставленной задачей выбирается опция блокирования трафика;

6. На последних двух страницах, страницах «**Профиль**» и «**Имя**» (**Profile, Name**), указываются профили (например, все), а также имя создаваемого правила, скажем, «**Block ICMP-v4**». После этого по нажатию на кнопку «**Готово**» (**Finish**) очередное правило будет создано.

Осталось проверить, правильно ли будет применяться такое правило. Для этого достаточно открыть окно командной строки и попробовать «пропинговать» какой-то адрес. Как видно на рисунке №1.13, мне не удалось этого сделать, что означает, что правило применилось без ошибок.

Применение правил только для избранных IP-адресов. Последний тип правила межсетевого экрана Windows, связан с областью применения такого правила. Другими словами, если вам необходимо, чтобы часть правил межсетевого экрана Windows распространялась только на отдельную группу компьютеров, вам не обязательно создавать для этого несколько объектов групповой политики и связывать их с различными подразделениями или указывать для каждого такого объекта свою область применения. Вы можете просто создать в одном объекте GPO ряд правил, в которых будет указана своя область применения.

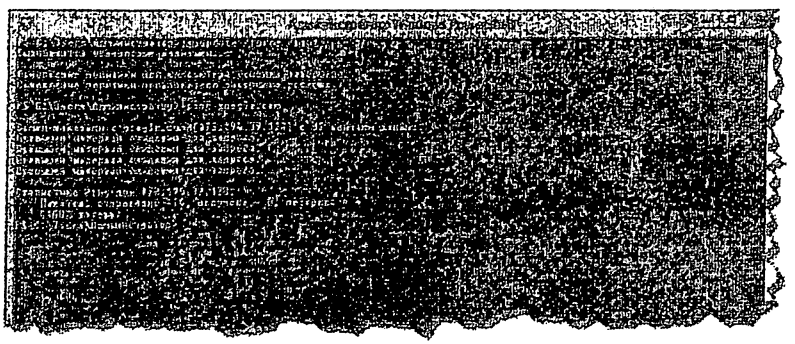


Рис. 1.13. Тестирование примененного правила межсетевого экрана Windows

В следующем примере будет продемонстрирована ситуация, в которой создается правило, блокирующее RDP-порт для компьютеров, локальные адреса которых входят в диапазон 10.1.1.112 – 10.1.1.130. Для создания такого правила нужно:

1. Находясь в узле **«Правила для исходящих подключений» (Outbound Rules)** редактора GPME, вызвать мастер создания правила для нового входящего подключения;

2. Как и в предыдущих двух описанных случаях из этого раздела, на первой странице мастера выбирается опция **«Настраиваемые» (Custom)**, после чего можно нажимать на кнопку **«Далее» (Next)**;

3. Так как зачастую пользователи используют для подключения к удаленному рабочему столу по порту 3389 программу **«Подключение к удаленному рабочему столу»**, на странице **«Программа» (Program)** желательно установить переключатель на опцию **«Путь программы» (This program path)** и в соответствующем текстовом поле ввести ***«C:WindowsSystem32mstsc.exe»*** без кавычек, а затем нажать на **«Далее» (Next)**;

4. На странице **«Протокол и порты» (Protocols and Ports)** следует из раскрывающегося списка **«Тип протокола» (Protocol type)** выбрать протокол TCP, а в раскрывающемся списке **«Локальный порт» (Local port)** оставить выбранной опцию **«Все порты» (Specific Ports)**;

5. Следующая страница – **«Область» (Scope)** – сейчас интересует нас больше всего. Как я успел упомянуть ранее, именно на этой странице мастера вы можете указать IP-адреса как для локальных, так и для удаленных компьютеров, на которые будут распространяться установленные в настоящем правиле ограничения.

6. Здесь, как заметно на рисунке №1.14, присутствуют два основных раздела для управления локальными и удаленными IP. Учтите, что в том случае, если IP-адрес локального компьютера будет фигурировать в списке локальных адресов, тогда весь входящий трафик от любого удаленного IP-адреса будет удовлетворять разрешениям, определенным в текущем правиле. На этой странице в случае как с локальными, так и с удаленными адресами, при выборе опции **«Любой IP-адрес» (Any IP address)** правило будет фильтровать сетевые пакеты с любым адресом, указанным в качестве локального IP-адреса, причем локальный компьютер будет всегда удовлетворять такому правилу. Если же вам нужно указать конкретные IP-адреса, установите переключатель на опцию **«Указанные IP-адреса»**

(**These IP addresses**) и укажите определенный адрес, диапазон адресов или подсеть, используя диалоговое окно, открывающееся по нажатию на кнопку «**Добавить**» (**Add**). Как также можно заметить на рисунке №1.14, при вызове диалогового окна добавления IP-адресов можно при установленном переключателе на первой опции «**IP-адрес или подсеть**» (**This IP address or subnet**) либо указать отдельный IP-адрес, либо целую подсеть компьютеров компании, а при установленном переключателе на опции «**Диапазон IP-адресов**» (**This IP address range**) указать только определенный диапазон таких адресов. Например, в данном случае, согласно поставленному ранее условию, следует установить переключатель на вторую опцию и в соответствующие поля «**с**» и «**по**» (**From, To**) ввести адреса 10.1.1.112 и 10.1.1.130.

Также можно отдельно выделить кнопку «**Настроить**» (**Customize**), отвечающую за настройку типов интерфейсов, к которым будет применяться создаваемое вами правило. Для выбора доступны три основных типа интерфейса, к которым относятся локальная сеть, а также удаленный или беспроводной доступ. Как вы видите, в данном случае из этого диалогового окна будут выбраны только первая и последняя позиции.

7. После этого идут известные по остальным примерам три страницы, на которых выбирается действие (в данном случае это блокировка подключения), профили, на которые будет распространяться такое правило (например, только доменный профиль), а также имя создаваемого правила (пусть это правило называется «**Block RDP for mstsc.exe**»). После того как будут определены все настройки для создаваемого правила, можно нажимать на кнопку «**Готово**» (**Finish**).

И в очередной раз необходимо протестировать получившиеся результаты. Для этого нужно взять компьютер, адрес которого входит в указанный в правиле диапазон, а затем открыть требуемое приложение и попробовать подключиться к удаленному рабочему столу. Как видно на

рисунке №1.15, в данном случае все было сделано правильно, и пользователю запрещается подключение:

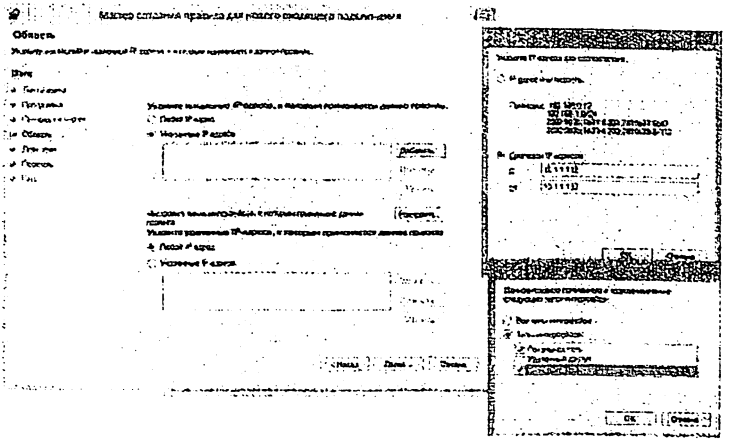


Рис. 1.14. Страница «Область» и диалоговые окна добавления IP-адресов с настройкой типов интерфейсов

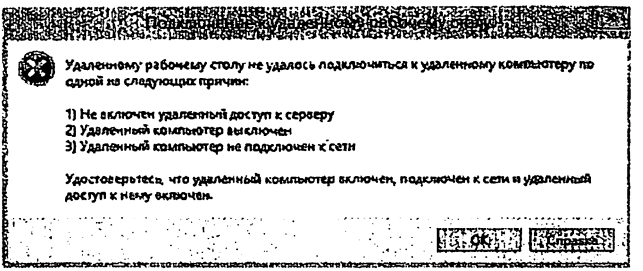


Рис. 1.15. Результаты тестирования последнего правила межсетевого экрана

По сути, эти типы правил представляют собой некий базис, необходимый для создания в будущем сложных корпоративных правил, удовлетворяющих различным бизнес-целям и потребностям.

Задание:

Настроить межсетевой экран в последовательности, указанной в практической части и изучить процедуру разработки политики межсетевого экрана

Контрольные вопросы:

1. Что такое межсетевой экран? Перечислите основные функции межсетевого экрана.
2. Как осуществляется формирование политики безопасности межсетевого экрана?
3. Какие настройки необходимо сделать в условиях, когда риски "низкие", "средние" и "высокие"?
4. Выделите основные типы межсетевых экранов.
5. Какие действия по умолчанию осуществляются межсетевым экраном в отношении трафика?
6. Как создается правило для программ? Какие профили можно выбрать к созидаемой правиле?
7. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора?
8. Почему порядок правил в наборе правил межсетевого экрана играет важную роль?

ПРАКТИЧЕСКАЯ РАБОТА №2.
СРЕДСТВА ОБНАРУЖЕНИЯ И ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ ПРОГРАММ.

Цель работы: Освоение практических навыков по формированию политики безопасности антивирусов и получение навыков по работе средств защиты от компьютерных вирусов и антивирусных программ

Теоретическая часть.

Политики защиты от вредоносных программ управляют параметрами действий и уведомлений при обнаружении вредоносных программ. Ниже перечислены важные параметры политик защиты от вредоносных программ.

1. **Действие.** Указывает, что делать, если сообщение содержит вредоносные программы. Доступны следующие варианты:

- Удаление сообщения (это значение по умолчанию).
- Замените все вложения текстовым файлом, который содержит этот текст по умолчанию: "В одном или нескольких вложениях этого сообщения электронной почты обнаружены вредоносные программы. Все вложения удалены".
- Замените все вложения текстовым файлом, который содержит настраиваемый текст.

2. **Уведомления.** Если политика антивирусных программ настроена для удаления сообщений, вы можете выбрать, отправлять ли сообщение уведомления отправите отправителю. Отправка уведомлений может зависеть от того, является ли отправитель внутренним или внешним. По умолчанию сообщение с уведомлением обладает следующими свойствами:

- *From:* Postmaster <*defaultdomain*> postmaster@.com
- *Тема:* неразличимое сообщение
- *Текст сообщения.* Это сообщение было создано автоматически с помощью программного обеспечения доставки почты. Ваше электронное сообщение не было доставлено получателям, так как в нем обнаружены вредоносные программы".

Вы можете настраивать свойства сообщений для внутренних и внешних уведомлений. Вы также можете указывать дополнительных получателей (администраторов), которые будут получать уведомления о недоставленных сообщениях от внутренних или внешних отправителей.

3. **Фильтры получателей.** Для настраиваемой политики противомалярийных программ можно указать условия и исключения получателей, которые определяют, к кому применяется политика. Для условий и исключений можно использовать следующие свойства:

- по получателю;
- по обслуживаемому домену;
- по членству в группе.

Условие или исключение можно использовать только один раз, но оно может содержать несколько значений. Указать несколько значений в одном условии или исключении можно с помощью оператора OR (например, *<recipient1>* or *<recipient2>*). Между разными условиями и исключениями используется оператор AND (например, *<recipient1>* and *<member of group 1>*).

4. **Приоритет.** Если вы создаете несколько настраиваемой политики противовирусных программ, вы можете указать порядок, который они применяются.

Простые вирусы могут быть легко обнаружены с помощью поиска сигнатуры (строк байт) около точки входа в программу, которая будет там присутствовать там после заражения программы вирусом. Полиморфные вирусы модифицируют себя в ходе размножения, поэтому их нельзя обнаружить с помощью сигнатуры, и обычно их выявляют с помощью выполнения программы в безопасной среде (среде виртуального процессора). Вирусы в загрузочных записях модифицируют эти загрузочные записи таким образом, что вирус будет выполняться при загрузке компьютера.

Приложения, которые поддерживают макросы, подвергают себя риску заражения макровирусами. Макровирусы - это команды, которые встроены в файлы вместе с данными. Примерами таких приложений являются Word, Excel и интерпретаторы Postscripta. Когда они открывают файлы данных, то происходит заражение макровирусом.

Политика безопасности для борьбы с вирусами имеет три составные части:

- Предотвращение - правила, позволяющие предотвратить заражение вирусами.
- Обнаружение - как определить, что данный выполняемый файл, загрузочная запись, или файл данных содержит вирус.

- Удаление - удаление вируса из зараженной компьютерной системы может потребовать переустановки ОС с нуля, удаления файлов, или удаления вируса из зараженного файла.

Имеется много различных факторов, важных при определении необходимого уровня защиты от заражения вирусами. Вирусы опасны при работе в DOS, Windows (3.X и 95) и NT. Кроме того, имеется ряд вирусов для Unix (в том числе для Linux).

Вероятность заражения вирусами пропорциональна частоте появления новых файлов или приложений на компьютере. Изменения в конфигурации для работы в Интернете, для чтения электронной почты и загрузка файлов из внешних источников - все это увеличивает риск заражения вирусами.

Чем больше значение компьютера или данных, находящихся в нем, тем больше надо позаботиться о мерах безопасности против вирусов. Нужно еще и учесть затраты на удаление вирусов из ваших компьютеров, а также из компьютеров ваших клиентов, которых вы можете заразить. Затраты не всегда ограничиваются только финансами, также важна и репутация организации, и другие вещи.

Важно также помнить, что вирусы обычно появляются в системе из-за действий пользователя (например, установки приложения, чтения файла по FTP, чтения электронного письма). Политика предотвращения может поэтому обращать особое внимание на ограничения на загрузку потенциально зараженных программ и файлов. В ней также может быть указано, что в среде с высоким риском проверка на вирусы особенно тщательно должна производиться для новых файлов.

Низкий риск. Политика контроля за импортом программ для Среды с низким риском должна в основном описывать меры по доведению до пользователей их обязанностей по регулярной проверке на вирусы.

Предотвращение: Пользователи должны знать о возможностях заражения вирусами и РПС из Интернета и о том, как использовать антивирусные средства.

Обнаружение: Коммерческие антивирусные средства могут использоваться для еженедельной проверки на вирусы. Ведение журналов работы антивирусных средств не является необходимым.

Сотрудники должны информировать системного администратора о любом обнаруженном вирусе, изменении конфигурации, или необычном поведении компьютера или программы. После получения информации об обнаружении вируса системный администратор должен информировать всех пользователей, имеющих доступ к программам или файлам данных, которые могли быть заражены вирусом, что возможно вирус заразил их системы. Пользователям должен быть сообщен порядок определения, заражена ли их система, и удаления вируса из системы. Пользователи должны сообщить о результатах проверки на вирусы и удаления вируса системным администраторам.

Удаление: Любая машина, которая подозревается в заражении вирусом, должна быть немедленно отключена от сети. Машина не должна подключаться к сети до тех пор, пока системные администраторы не удостоверятся в удалении вируса. По возможности должны использоваться коммерческие антивирусные программы для удаления вируса. Если такие программы не могут удалить вирус, все программы в компьютере должны быть удалены, включая загрузочные записи при необходимости. Все эти программы должны быть повторно установлены из надежных источников и повторно проверены на вирусы. (В России зарегистрированные пользователи могут обратиться по электронной почте к фирме-производителю программы и получить обновление программы со средствами удаления вируса).

Средний риск. Политика контроля за импортом программ для Среды со средним риском должна требовать более частых проверок на вирусы, и

использования антивирусных программ для проверки серверов и электронной почты.

Предотвращение: Программы должны загружаться и устанавливаться только сетевым администратором (который проверяет их на вирусы или тестирует).

На файловые сервера должны быть установлены антивирусные программы для ограничения распространения вирусов в сети. Должна производиться ежедневная проверка всех программ и файлов данных на файловых серверах на вирусы. Рабочие станции должны иметь резидентные в памяти антивирусные программы, сконфигурированные так, что все файлы проверяются на вирусы при загрузке на компьютер. Все приходящие электронные письма должны проверяться на вирусы. Запрещается запускать программы и открывать файлы с помощью приложений, уязвимых к макровирусам, до проведения их проверки на вирусы.

Программа обучения сотрудников компьютерной безопасности должна содержать следующую информацию о риске заражения вирусами:

Антивирусные программы могут обнаружить только те вирусы, которые уже были кем-то обнаружены раньше. Постоянно разрабатываются новые, более изощренные вирусы. Антивирусные программы должны регулярно обновляться (ежемесячно или ежеквартально) для того, чтобы можно было обнаружить самые новые вирусы. Важно сообщать системному администратору о любом необычном поведении компьютера или приложений. Важно сразу же отсоединить компьютер, который заражен или подозревается в заражении, от сети, чтобы уменьшить риск распространения вируса.

Обнаружение: Должны использоваться коммерческие антивирусные программы для ежедневных проверок на вирусы. Антивирусные программы должны обновляться каждый месяц. Все программы или данные, импортируемые в компьютер (с дискет, электронной почты и т.д.) должны проверяться на вирусы перед их использованием.

Журналы работы антивирусных средств должны сохраняться и просматриваться системными администраторами. Сотрудники должны информировать системного администратора об обнаруженных вирусах, изменениях в конфигурации или странном поведении компьютера или приложений.

При получении информации о заражении вирусом системный администратор должен информировать всех пользователей, которые имеют доступ к программам и файлам данных, которые могли быть заражены вирусом, что вирус возможно заразил их системы. Пользователям должен быть сообщен порядок определения, заражена ли их система, и удаления вируса из системы. Пользователи должны сообщить о результатах проверки на вирусы и удаления вируса системным администраторам.

Удаление: Любая машина, которая подозревается в заражении вирусом, должна быть немедленно отключена от сети. Машина не должна подключаться к сети до тех пор, пока системные администраторы не удостоверятся в удалении вируса. По возможности должны использоваться коммерческие антивирусные программы для удаления вируса. Если такие программы не могут удалить вирус, все программы в компьютере должны быть удалены, включая загрузочные записи при необходимости. Все эти программы должны быть повторно установлены из надежных источников и повторно проверены на вирусы.

Высокий риск. Системы с высоким уровнем риска содержат данные и приложения, которые являются критическими для организации. Заражение вирусами может вызвать значительные потери времени, данных и нанести ущерб репутации организации. Из-за заражения может пострадать большое число компьютеров. Следует принять все возможные меры для предотвращения заражения вирусами.

Предотвращение: Администратор безопасности должен разрешить использование приложений перед их установкой на компьютер. Запрещается устанавливать неавторизованные программы на компьютеры.

Конфигурации программ на компьютере должны проверяться ежемесячно на предмет выявления установки лишних программ.

Программы должны устанавливаться только с разрешенных внутренних серверов для ограничения риска заражения. Нельзя загружать программы с Интернета на компьютеры. С помощью Межсетевого экрана должна быть запрещена операция GET (загрузка файла) с внешних серверов.

На файловые сервера должны быть установлены антивирусные программы для ограничения распространения вирусов в сети. Должна производиться ежедневная проверка всех программ и файлов данных на файловых серверах на вирусы. Рабочие станции должны иметь резидентные в памяти антивирусные программы, сконфигурированные так, что все файлы проверяются на вирусы при загрузке на компьютер. Запрещается запускать программы и открывать файлы с помощью приложений, уязвимых к макровирусам, до проведения их проверки на вирусы.

Все приходящие письма и файлы, полученные из сети, должны проверяться на вирусы при получении. По возможности проверка на вирусы должна выполняться на межсетевом экране, управляющем доступом к сети. Это позволит централизовать проверку на вирусы для всей организации и уменьшить затраты на параллельное сканирование на рабочих станциях. Это также позволит централизовать администрирование антивирусных программ, ограничить число мест, куда должны устанавливаться последние обновления антивирусных программ.

Программа обучения сотрудников компьютерной безопасности должна содержать следующую информацию о риске заражения вирусами:

Антивирусные программы могут обнаружить только те вирусы, которые уже были кем-то обнаружены раньше. Постоянно разрабатываются новые, более изощренные вирусы. Антивирусные программы должны регулярно обновляться (ежемесячно или ежеквартально) для того, чтобы можно было обнаружить самые новые вирусы. Важно сообщать системному

администратору о любом необычном поведении компьютера или приложений. Важно сразу же отсоединить компьютер, который заражен или подозревается в заражении, от сети, чтобы уменьшить риск распространения вируса.

Несоблюдение данной политики должно вести к наказанию сотрудника согласно стандартам организации.

Обнаружение: Все программы должны быть установлены на тестовую машину и проверены на вирусы перед началом их использования в рабочей среде. Только после получения разрешения администратора безопасности можно устанавливать программы на машинах сотрудников.

Помимо использования коммерческих антивирусных программ, должны использоваться эмуляторы виртуальных машин для обнаружения полиморфных вирусов. Все новые методы обнаружения вирусов должны использоваться на этой тестовой машине. Антивирусные программы должны обновляться ежемесячно или при появлении новой версии для выявления самых новых вирусов.

Проверка всех файловых систем должна производиться каждый день в обязательном порядке. Результаты проверок должны протоколироваться, автоматически собираться и анализироваться системными администраторами.

Все данные, импортируемые на компьютер, тем или иным способом (с дискет, из электронной почты и т.д.) должны проверяться на вирусы. Сотрудники должны информировать системного администратора об обнаруженных вирусах, изменениях в конфигурации или странном поведении компьютера или приложений.

При получении информации о заражении вирусом системный администратор должен информировать всех пользователей, которые имеют доступ к программам и файлам данных, которые могли быть заражены вирусом, что вирус возможно заразил их системы. Пользователям должен

быть сообщен порядок определения, заражена ли их система, и удаления вируса из системы.

Удаление: Любая машина, которая подозревается в заражении вирусом, должна быть немедленно отключена от сети. Машина не должна подключаться к сети до тех пор, пока системные администраторы не удостоверятся в удалении вируса. По возможности должны использоваться коммерческие антивирусные программы для удаления вируса. Если такие программы не могут удалить вирус, все программы в компьютере должны быть удалены, включая загрузочные записи при необходимости. Все эти программы должны быть повторно установлены из надежных источников и повторно проверены на вирусы.

Практическая часть.

На практической части данной работы на примере «Политики антивирусной программы» Департамента информатизации изучим как составлять Политику антивирусных программ.

Политика антивирусных программ состоит из следующих разделов:

1. Термины и определения
2. Основные положения
3. Общие требования
4. Ответственность.

1. Термины и определения.

Термины, определения и сокращения, применяемые в настоящем документе, используются в соответствии с документом ОИБ-ТО/3.13/001 «Термины и определения».

2. Основные положения.

2.1. Настоящий документ «Политика антивирусной защиты» далее - Политика) - определяет систему мер, направленных на защиту инфраструктуры информационных систем КСПД ТО от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (троянских программ,

логических бомб и т.п.), а также устанавливает единые требования к организации системы антивирусной защиты информационных систем и всех типов автоматизированных рабочих мест, требования к конфигурации применяемых программных средств и процедуры их эксплуатации.

2.2. Реализация требований Политики производится лицами, назначенными в установленном порядке администраторами информационной безопасности ИОГВ либо подразделением (или организацией), привлекаемым для выполнения данных функций.

2.3. Политика подлежит регулярному пересмотру с периодичностью 1 раз в год для проведения системы защиты в соответствие реальным условиям. Также может проводиться внеплановый пересмотр при изменения перечня решаемых задач, конфигурации технических и программных средств.

2.4. Настоящая Политика:

- определяет единые требования по организации антивирусной защиты во всех информационных системах и отдельные АРМ, входящих в состав или подключенных к КСПД ТО;
- определяет необходимые и достаточные меры антивирусной защиты для поддержания бесперебойной и безопасной работы пользователей КСПД ТО;
- определяет распределение административных ролей сотрудников Участников процессов ИБ при организации антивирусной защиты объектов КСЦД ТО;
- определяет обязанности пользователей КСПД ТО и администраторов информационной безопасности ИОГВ в рамках организации антивирусной защиты;
- применяется ко всем информационным системам и отдельные АРМ, подключенные к КСПД ТО;

- обязательна к исполнению всеми партнерами, исполнителями по заключенным с Участниками процессов ИБ контрактам/ договорам и другими лицами, и организациями, постоянно использующим или имеющим периодическое подключение к сетевым или информационным ресурсам КСПД ТО.

3. Общие требования.

3.1. Запрещено использование в процессе нормальной (штатной) эксплуатации информационных систем программного обеспечения, программных кодов или алгоритмов, приводящих к разрушению, уничтожению информационных ресурсов.

3.2. Методы борьбы с вредоносным программным обеспечением должны включать в себя три составные части:

- Предотвращение — действия, позволяющие предотвратить заражение вредоносным программным обеспечением;
- Обнаружение — методология определения наличия вредоносного программного обеспечения;
- Удаление — физическое удаление кодов вредоносного программного обеспечения из зараженных файлов или зараженной системы.

3.3. К использованию в информационных системах, входящих в состав КСПД ТО, допускаются только лицензионные антивирусные средства, разрешенные для применения в органах власти РФ.

3.4. Все сервера, рабочие станции и прочие технологические сервисы и системы обеспечиваются в обязательном порядке средствами антивирусной защиты, если используемая на них операционная система имеет вирусную уязвимость.

3.5. Актуализация версий используемых антивирусных средств и антивирусных баз проводится на регулярной основе.

3.6. Системные администраторы серверов и администраторы ресурсов должны постоянно поддерживать максимально возможный уровень

безопасности вверенных им программно-технических средств. Для этого необходимо:

- отслеживать информацию, поступающую от разработчиков системного и программного обеспечения об обнаруженных ошибках и уязвимостях;
- своевременно устанавливать официально рекомендуемые разработчиками системного и прикладного программного обеспечения обновления и исправления;
- отключить все неиспользуемые сервисы и приложения операционной системы (или прикладного ПО);
- поддерживать в актуальном состоянии установленные средства антивирусной защиты.
- вести журналы системных событий и регулярно анализировать их;
- следовать рекомендациям администратора информационной безопасности ИОГВ.
- Загрузка программного обеспечения и рабочих файлов на компьютеры, сервера и прочие носители информации осуществляется с проведением предварительной их проверки антивирусными средствами.

3.7. Загрузка программного обеспечения и рабочих файлов на компьютеры, сервера и прочие носители информации осуществляется с проведением предварительной их проверки антивирусными средствами.

3.8. Пользователям запрещается самостоятельная установка и использование специализированного программного обеспечения без предварительного согласования с администратором информационной безопасности ИОГВ.

3.9. Установка разрешенных средств антивирусной защиты на компьютеры пользователей осуществляется администраторами

информационной безопасности ИОГВ, имеющими соответствующие полномочия.

3.10. Пользователям КСПД ТО запрещается отключать установленные на компьютерах средства антивирусной защиты или производить изменения их конфигурации, снижающие установленный уровень защиты.

4. Ответственность

4.1. За общее состояние централизованных средств антивирусной защиты в КСПД ТО отвечает ГКУ ТО «Центр информационных технологий Тюменской области» - Администратор Информационной безопасности исполнительные органов государственной власти Тюменской области.

4.2. Сотрудники Участников процессов ИБ несут персональную ответственность за соблюдение требований настоящей Политики.

4.3. Сотрудники сторонних организаций, выполняющих работы в интересах Участников процессов ИБ, несут ответственность за безопасность разрабатываемого ими программного обеспечения от воздействия существующих вирусов и от наличия в них самих фрагментов кодов, приводящих к разрушению или уничтожению информационных ресурсов.

4.4. Партнеры и сторонние организации, подключенные к линиям связи или использующие информационные ресурсы КСПД ТО и ГСПД на основании имеющихся соглашений и договоров, несут ответственность за применение, использование или распространение вредоносного программного обеспечения в отношении программно-технических средств и информационных ресурсов в соответствии с действующим законодательством Российской Федерации.

Задание:

Изучить процедуру разработки политики антивирусных программ и формировать политику в последовательности указанной в практической части на примере организации

Контрольные вопросы:

1. Как осуществляется формирование политики безопасности антивирусных программ?
2. Какие разделы включает в себя политика антивирусных программ?
3. Можно ли указать порядок если создать несколько настраиваемой политики противовирусных программ?
4. Какие настройки необходимо сделать в условиях, когда риски "низкие", "средние" и "высокие"?
5. Какие составные части должны включать в себя методы борьбы с вредоносным программным обеспечением?

ПРАКТИЧЕСКАЯ РАБОТА №3.

ЗАЩИТА УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ С ПОМОЩЬЮ GOOGLE AUTHENTICATOR.

Цель работы: Освоение знаний и практических навыков о методах аутентификации пользователей, порядке построения политики аутентификации пользователей в сети и по защите учетных записей пользователей с помощью Google Authenticator.

Теоретическая часть.

Ряд вопросов возникает после того, как вы узнали про необходимость обеспечения той или иной комбинации бизнес-требований для работы в киберпространстве. Какие программно-аппаратные средства и организационные меры должны быть реализованы, чтобы удовлетворить потребности организации? Каков наш профиль риска? Каковы должны быть

наши этические нормы для того, чтобы организация могла решать свои задачи с помощью Интернета? Кто за что должен отвечать? Основа ответов на подобные вопросы - это концептуальная политика безопасности для организации.

Политики безопасности можно разделить на две категории - технические политики, реализуемые с помощью оборудования и программ, и административные политики - выполняемые людьми, использующими систему и людьми, управляющими ей.

В этой практической работе вы узнаете об управлении проверкой подлинности пользовательских учетных записей, а именно об узле «*Политики учетных записей*». Применение этих политик распространено в предприятиях с доменной средой. Для обеспечения безопасности ваших компьютеров, применение политик этой группы на компьютерах, не входящих в доменную среду (например, использование политик на вашем домашнем компьютере) поможет вам существенно повысить безопасности компьютера.

Без сомнения, корпоративные учетные записи представляют огромный интерес для хакеров, которых может заинтересовать хищение корпоративной информации, а также получение доступа к компьютерам вашего предприятия. Поэтому, одним из решений, позволяющих существенно обезопасить инфраструктуру предприятия, является использование безопасных сложных паролей для снижения возможности проникновения злоумышленниками.

Общие политики аутентификации в Интернете. Хотя пароли легко скомпрометировать, организация может посчитать, что угроза маловероятна, что восстановление после инцидента будет несложным и что инцидент не затронет критические системы (на которых могут иметься другие механизмы защиты).

Низкий риск. Требуется аутентификация для доступа к системам организации из Интернета. Минимальным стандартом для аутентификации

является использование паролей, как описано в политике паролей ОС Windows.

Средний риск. Доступ к информации класса XXX и ее обработка из Интернета (при ее несанкционированной модификации, раскрытии или уничтожении имеет место небольшой ущерб) требует использования паролей, а доступ ко всем остальным видам ресурсов требует использования устойчивой аутентификации.

Доступ в режиме telnet к корпоративным ресурсам из Интернета требует использования устойчивой аутентификации.

Высокий риск. Доступ из Интернета ко всем системам за межсетевым экраном требует использования устойчивой аутентификации. Доступ к информации XXX и ее обработка (при нарушении ее безопасности организация понесет большой ущерб) требует использования постоянной аутентификации.

Если вы решили использовать устойчивую аутентификацию, то вам требуется понимать за счет чего достигается безопасность и учитывать затраты на обучение пользователей и дополнительное администрирование. Пользователи будут гораздо более грамотно использовать средства аутентификации, если они соответствующим образом обучены, как их использовать и им объяснено, почему нужно применять именно их.

Существует много технологий для реализации устойчивой аутентификации, включая генераторы динамических паролей, системы запрос-ответ на основе криптографии и смарт-карт, а также цифровые подписи и сертификаты. При использовании электронных подписей и сертификатов возникают новые вопросы - каковы требования обеспечения безопасности для сертификатов?

Пользователи устойчивой аутентификации должны прослушать курсы перед началом применениями ими этого метода аутентификации.

Сотрудники отвечают за безопасное использование и хранение всех устройств аутентификации, принадлежащих организации. Смарт-карты не

должны храниться вместе с компьютером, используемым для доступа к компьютерам организации. При утере или краже смарт-карты о случившемся надо немедленно сообщить службе безопасности, чтобы можно было заблокировать его использование.

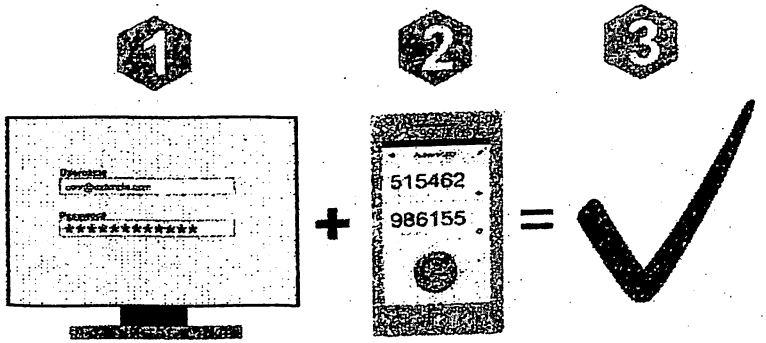
В наши дни, скорее всего, уже у каждого есть по крайней мере одна или две учетные записи для хранения огромного количества конфиденциальной информации и личных данных, от электронной почты до биометрических и банковских данных. В связи с этим, защита этих учетных записей должна быть в приоритете у каждого пользователя мобильного устройства. В дополнение к надежному паролю одним из самых безопасных и все более распространенных способов защиты ваших учетных записей и устройств является двухфакторная аутентификация.

Двухфакторная аутентификация (2fa code) — это метод подтверждения права доступа юзера к учетной записи того или иного веб-сервиса с помощью системы одноразовых паролей.

Настройка 2FA — это включение дополнительных факторов для входа в систему. Например, с помощью смс, отпечатков пальца при помощи специального устройства или шестизначного кода Google Authenticator (GA) о котором мы и расскажем в данной работе.

Что такое шестизначный код GA — это одноразовый пароль, который постоянно генерируется в течение 30 секунд. За это время его нужно будет успевать ввести в поле при входе на биржу или в другие системы, где у вас стоит защита 2FA. Это шестизначный код генерируется даже при отключенном интернете.

Существует несколько вариантов практической реализации данного метода защиты аккаунта. В этом обзоре мы рассмотрим настройку специального приложения для генерации случайных кодов Google Authenticator. Эта программа была разработана для защиты учетных записей Google, но получила широкое применение на крипто валютных биржах и других ресурсах.



Google Authenticator используется как второй уровень защиты при входе в личный кабинет или выводе средств с торговой площадки, а на некоторых биржах даже и при формировании ордеров.

Программа, установленная на ваш мобильный девайс, создает каждые 30 секунд шестизначный цифровой пароль. Для подтверждения входа или другой операции вы должны ввести его в формуляр запроса. Если код прошел проверку на валидность, ваши права доступа подтверждены. Порядок активации Google Authenticator идентичен для всех веб-ресурсов.

Таким образом, двухэтапная аутентификация в настоящее время считается одним из лучших инструментов для защиты любого сервиса, приложения или социальной сети, которые вы используете, поэтому его основная функция - создать уровень безопасности, который очень трудно нарушить.

Следует отметить, что это довольно простое в использовании приложение, которое было очень полезно для пользователей, и что не имеет много функций помимо предоставления защита доступа к приложению, социальным сетям и другие услуги. Также есть возможность импорт или экспорт счетов прямо из приложения. Эта новая функция позволит пользователям выбирать, какую учетную запись экспортировать и, таким образом, создавать QR код. Хотя следует иметь в виду, что этот код не сохраняется, но цель состоит в том, чтобы использовать другое устройство

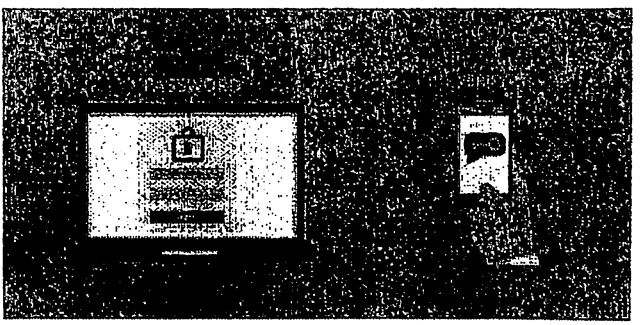
с приложением, чтобы иметь возможность сканировать и импортировать эти учетные записи.

Таким образом, эта функция стала очень простой возможностью переноса Google Authenticator с одного смартфона на другой. Важно помнить, что для того, чтобы воспользоваться этой новой функцией экспорта или импорта учетных записей, вы должны иметь установлена версия 5.1 на обоих устройствах, так как это будет единственный способ завершить эту процедуру.

Практическая часть.

На практической части этой работы продемонстрировано как создать и настроить Google Authenticator. Учитывая важность активации этой услуги для каждой из ваших учетных записей, мы покажем вам, как настроить этот сервис Google с вашими учетными записями в социальных сетях и на других платформах.

Подробная инструкция по активации Google Authenticator, как работает схема защиты, и что необходимо для ее функционирования. В качестве наглядного примера выберем самую крупную и популярную криптобиржу Binance.



В первую очередь зарегистрируйтесь на сайте https://www.binance.com. В принципе на любой серьезной крипто бирже есть инструкция по настройке двухфакторной аутентификации с помощью

Google Authenticator, мы просто изложим ее в общих чертах, чтобы начинающие трейдеры были заранее подготовленными.

Для подключения и настройки 2fa code понадобится смартфон или планшет с установленным приложением и доступ к учетной записи.

1. Заходим на настройки аккаунта Google и переходим на параметры безопасности. Для этого можно воспользоваться следующей ссылкой: myaccount/google/com/security/. У вас откроется следующее окно (Рис №3.1). Тут нужно включить параметры двухэтапной аутентификации.

2. Для включения этого параметра требуется подтверждение входа в учетную запись Google на персональном компьютере (Рис №3.2).

3. Далее переходим к изменению номера в приложении Google Authenticator (Рис №3.3).

4. После этого предстоит выбор типа устройства для подключения Google Authenticator исходя вашей модели телефона (Рис №3.4).

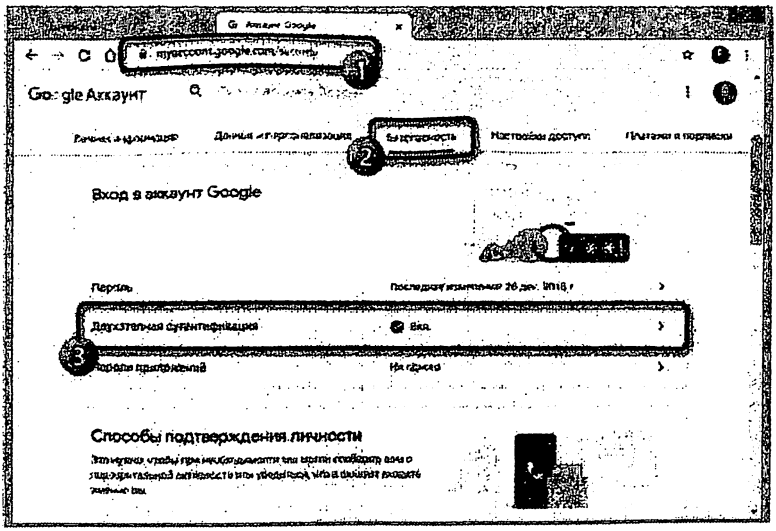


Рис 3.1. Переход к разделу двухэтапная аутентификация в настройках Google.

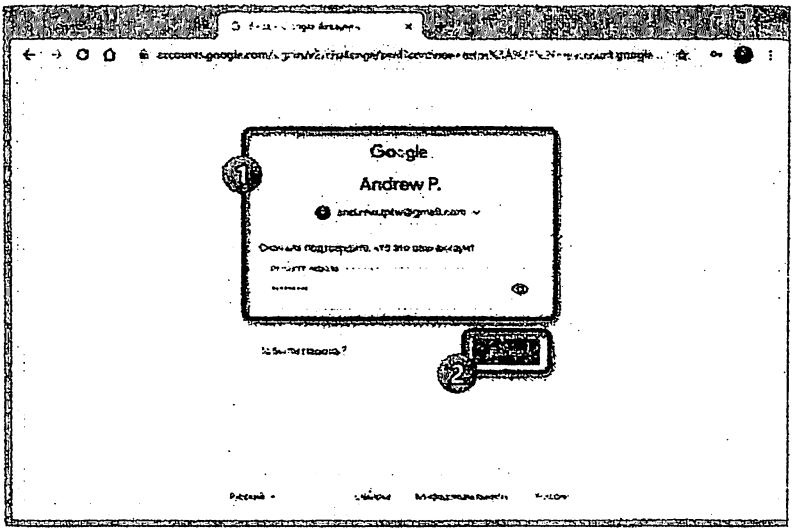


Рис № 3.2. Подтверждение входа в учетную запись Google на ПК.

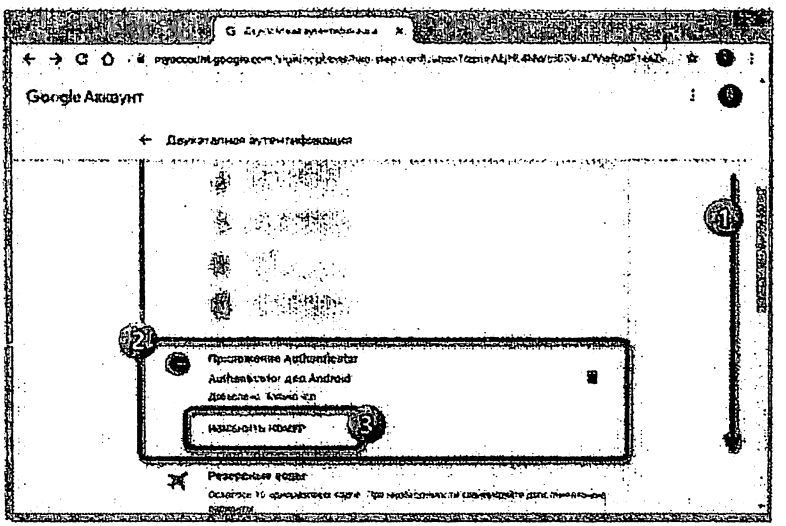


Рис. 3.3. Переход к изменению номера в приложении Google Authenticator.

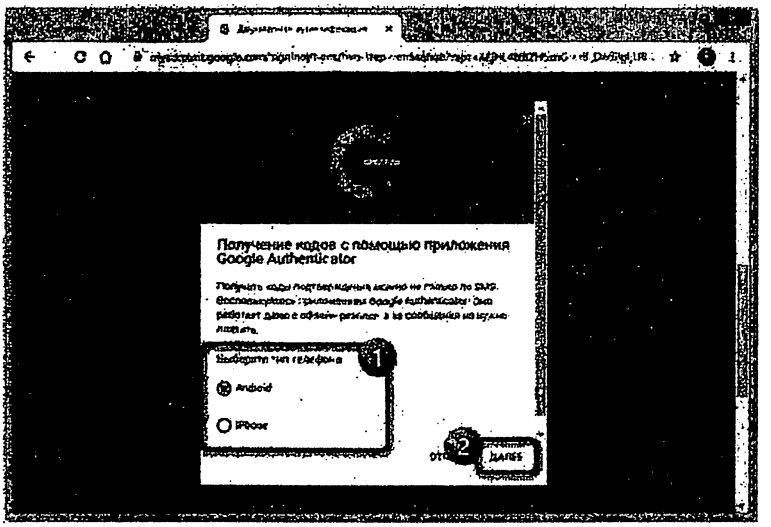


Рис. 3.4. Выбор типа устройства для подключения приложения Google Authenticator.

5. Чтобы настроить приложение Google Authenticator нужно пройти по официальным ссылкам и скачать его (Рис 3.5):

- Google Authenticator для iOS (iPhone, iPad) — https://apps.apple.com/
- Google Authenticator для Android — https://play.google.com/

Если у вас девайс на базе Android откройте Google Play Market и найдите там Google Authenticator, ну а счастливому владельцу продукции компании Apple нужно совершить аналогичное действие в App Store. Можно загрузить файл apk (for Android) с другого источника, но это не самый надежный вариант.

6. Сервис выведет QR-код и резервный ключ. Откройте Google Authenticator и нажмите символ фотоаппарата, чтобы программа отсканировала штрих-код (Рис. №3.6). Переходим к подключению кода для подключения приложения Google Authenticator с помощью штрих-кода (Рис.№ 3.7).

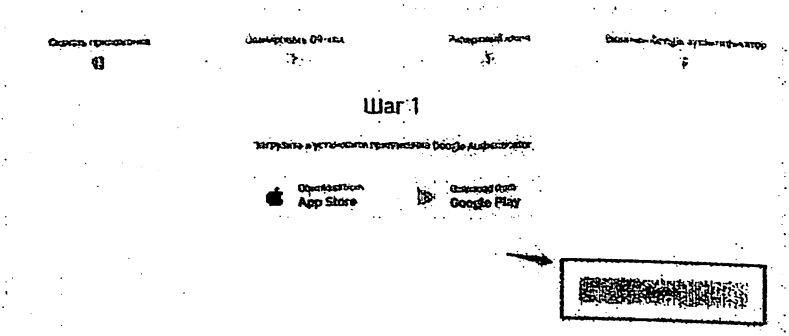


Рис. 3.5. Загрузка и установка Приложения Google Authenticator

7. Если по каким-то причинам произошел сбой, например, у вас не работает камера, введите 16-значный ключ 2FA в интерфейсе приложения на смартфоне и нажмите кнопку «Добавить». Неважно добавили вы аккаунт автоматически или вручную, ни в коем случае не забудьте сохранить в надежном месте (желательно на бумаге) код подключения (Рис.№3.8).

8. После этого появляется следующее окно. Это уведомления о том, что аутентификатор был включен успешно (Рис.№3.9).

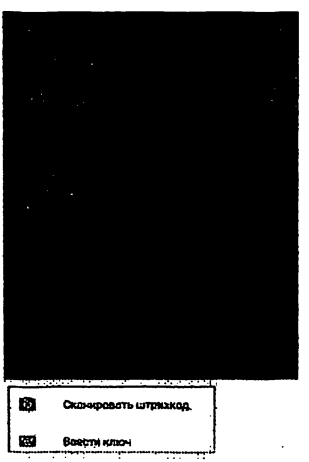


Рис. 3.6. Сканировать штрих-код

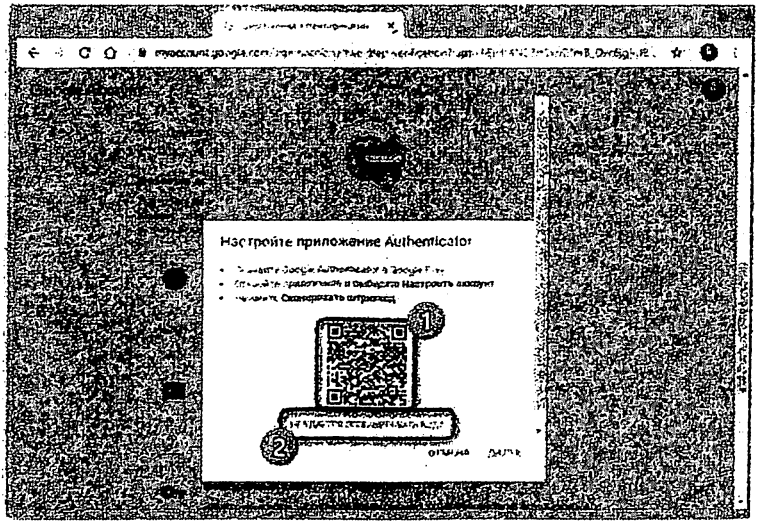


Рис. 3.7. Переход к подключению кода для подключения приложения Google Authenticator.

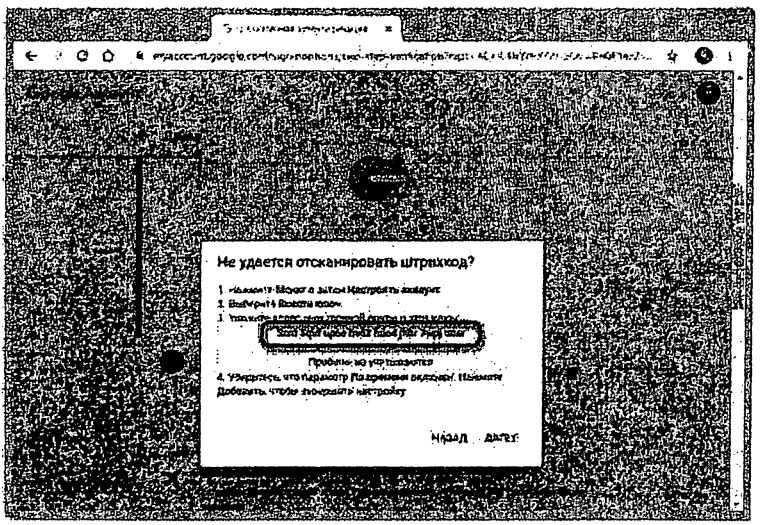


Рис.3.8. Введение 16-значного ключа 2FA в интерфейсе приложения на смартфоне

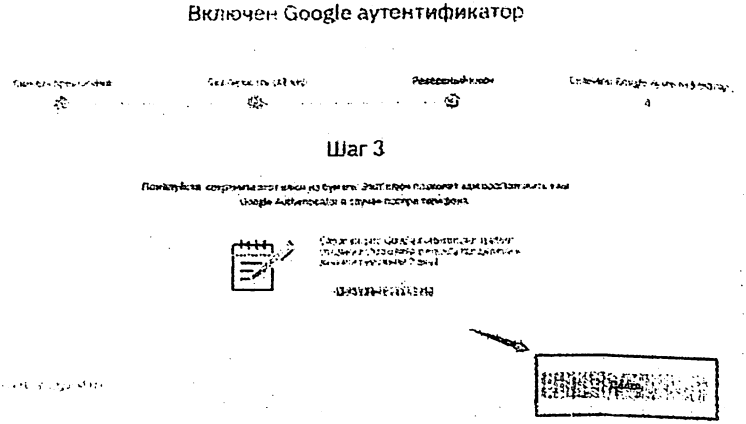


Рис. 3.9. Успешное подключение кода для подключения приложения Google Authenticator.

Создание пароля приложения Google Authenticator. Пароль приложения представляет собой 16-значный код доступа, который дает приложению или устройству разрешение на доступ к вашему аккаунту Google.

Если вы используете двухэтапную аутентификацию и видите ошибку "неправильный пароль" при попытке войти в свою учетную запись Google, пароль приложения может решить проблему. В большинстве случаев вам нужно будет вводить пароль приложения только один раз для каждого приложения или устройства, поэтому не беспокойтесь о его запоминании.

- Нажмите на ссылку "паролей приложений" в секции "Пароль и способ входа в аккаунт" страницы настройки безопасности аккаунта Google. Вас могут попросить войти в свой аккаунт Google.
- Внизу в выпадающем списке выберите приложение, которое вы используете.

- В следующем выпадающем списке выберите устройство, которое вы используете.
- Нажмите кнопку "Создать".
- Следуйте инструкциям, чтобы ввести пароль приложения (16-значный код в желтой строке) на устройстве.
- Нажмите "Готово".

Восстановление Google Authenticator при потере телефона. Если у вас активирована двухфакторной аутификации, то, потеряв свой смартфон, вы потеряете и доступ к учетной записи. Записали 16-значный ключ 2FA — прекрасно, нет никаких проблем.

Скачайте программу для двухфакторной аутентификации на другое устройство и добавьте аккаунт вручную. Но если у вас кода восстановления все намного сложнее. Пользователи, прошедшие полную верификацию на бирже, могут обратиться в **службу поддержки** и там им объяснят, как восстановить гугл аутентификатор. Ну а если вы работаете инкогнито, то сбросить настройки аутентификации Google, можно следующим образом:

- Откройте страницу входа.
- Укажите адрес электронной почты и пароль.
- Когда вас попросят ввести 2fa code, нажмите «**Не можете получить доступ к Google Authenticator?** ».
- Ознакомьтесь с напоминанием и подтвердите запрос на ликвидацию двухфакторки в окне сайта.
- Перейдите в почтовый ящик, откройте письмо с биржи и нажмите «**Confirm reset/ Подтвердить сброс**».

Теперь пройти полную верификацию личности и только после этого вы сможете заново активировать двухфакторную аутентификацию. Пока вы этого не сделаете ваш биржевой депозит будет заблокирован.

Кроме этого классического способа подключения Google Authenticator существуют методы подключения через другие учетные записи такие как, Facebook, Instagram, Pay Pal или Twitter.

Задание:

Настроить сервис Google Authenticator с вашими учетными записями в социальных сетях и на других платформах (Facebook, Instagram)

Контрольные вопросы:

1. Как осуществляется формирование политики безопасности учетных записей?
2. Какие настройки необходимо сделать в условиях, когда риски "низкие", "средние" и "высокие"?
3. Что такое шестизначный код GA?
4. Настройка 2FA это?
5. Как настроить сервис Google Authenticator с вашими учетными записями в социальных сетях и на других платформах?

ПРАКТИЧЕСКАЯ РАБОТА №4. ИСПОЛЬЗОВАНИЕ ПОЛЬЗОВАТЕЛЯМИ ИНСТРУМЕНТЫ УПРАВЛЕНИЯ ПАРОЛЯМИ.

Цель работы: Преобретение теоретических и практических навыков о политике паролей, об использовании пользователями инструменты управления паролями и по настройке менеджера паролей с помощью браузера, а также с посредством специальных программ.

Теоретическая часть.

Политика безопасности должна быть тесно связана с повседневным использованием Интернета сотрудниками организации и повседневным управлением сетью, и компьютерами. Она также должна быть интегрирована в культуру организации посредством обучения. Этот документ в основном описывает технические стороны политики. Но административные вопросы, такие как распределение обязанностей за поддержание безопасности, порой более важны. Эта практическая работа описывает дополнительные аспекты безопасности в киберпространстве,

которые должны быть учтены с помощью организационных мер, таких как политика пароля.

Политика паролей.

Парольная политика состоит из следующих разделов и разрабатывается примерно таким образом.

1. ***Описание.*** Пароли - один из важнейших аспектов информационной безопасности, так как плохо подобранный пароль повышает потенциальный риск несанкционированного доступа в информационную систему компании. Все сотрудники «ВАША КОМПАНИЯ» (включая подрядчиков и третью сторону) несут ответственность за выполнение требований настоящей политики.

2. ***Цель.*** Цель этой политики установить стандарты создания сильных паролей, их защиту, хранение и частоту изменения.

3. ***Область применения.*** Эта политика относится ко всему персоналу, кто имеет или ответственен за доступ к конфиденциальной информации всех уровней (или любая форма доступа, которая поддерживает или требует пароля) на любой системе, оборудовании, имеющем доступ (или хранящем конфиденциальную информацию) к Вашей корпоративной сети.

4. ***Политика.***

- Пароли системных учетных записей (администратора домена, локального администратора, root и т. д.) должны изменяться ежеквартально.
- Все пароли системных учетных записей, а также пароли приложений и активного оборудования необходимо хранить в базе данных в зашифрованном виде, доступ к которой ограничен.
- Срок действия паролей учетных записей домена должен составлять не более 9 месяцев. Рекомендуемый интервал смены пароля 6 месяцев.

- Пароль учетной записи пользователя, имеющего административные привилегии, полученные при помощи членства в группе или при помощи программ, таких как sudo, должен быть уникален по отношению к другим паролям учетных записей данного пользователя.
- Запрещается передача паролей пользователям при помощи почтовых сообщений либо иным другим открытым способом через Интернет.
- Пароль полученный пользователем, необходимо сменить при первом входе в систему.
- При использовании SNMP протокола, необходимо использовать отличные от стандартных значений строк подключений (Community Name) «public», «private», «system» и отличными от пароля используемого для входа в систему.
- Все пароли пользователей, а также системные пароли должны соответствовать данной политике.

5. ***Инструкции.*** Инструкция по созданию пароля. *«ВАША КОМПАНИЯ»* использует пароли для различных целей. Среди них: доступ к учётной записи пользователя, к веб-интерфейсам, к электронной почте, для защиты хранителя экрана, пароли голосовой почты и доступ к маршрутизаторам. Поскольку очень мало систем поддерживают токены с одноразовыми паролями (динамические пароли, которые используются только один раз), следует знать как выбрать стойкий пароль.

Плохие, слабые пароли обладают следующими признаками:

1. Содержат менее восьми символов.
2. Являются словом, которое содержится в словарях (русских или иностранных).
3. Являются частоупотребляемым словом.
4. Содержат фамилию, кличку животного, имена друзей, сотрудников, вымышленных персонажей и т. д.

5. Содержат компьютерные термины и названия, команды, названия сайтов, компаний, оборудования, программного обеспечения.
6. Содержат название вашей компании и географические наименования, например «Москва», «Саратов» или их производные.
7. Содержат даты рождения и иную личную информацию, например, адреса и номера телефонов.
8. Слово или число по шаблону типа аааббб, qwerty, zyxwvuts, 12345 и т.д.
9. Предыдущий пример, вводимый в обратной последовательности.
10. Два предыдущих примера с цифрой в начале или конце пароля (например, Москва1, 1Саратов).

6. Параметры сильных паролей.

1. Содержит сочетание букв верхнего и нижнего регистров (например, a-z, A-Z).
2. Включает цифры и знаки пунктуации, например, 0-9, !@#$%^&*()_+|~-=\`{}[[ ]]:«;'<>?,./).
3. Состоит из восьми и более символов.
4. Не является словом на любом языке, диалекте, сленге, жаргоне и т.д.
5. Не основан на пресональной информации, например фамилии, дате рождения и т.д.
6. Никогда не записывается и не хранится on-line.

Создавайте легкозапоминаемые пароли. Одним из способов создания таких паролей, использовать песни, стихи и другие легкозапоминающиеся фразы. Например из фразы: «This May Be One Way To Remember» можно получить такие пароли: «TmB1w2R!» или «Tmb1W>r~» и другие варианты.

7. Правила парольной защиты.

1. Не используйте один и тот же пароль для доступа к учётным записям *«ВАША КОМПАНИЯ»* и к другим ресурсам (например, доступ в интернет из дома, системам электронной коммерции и т. д.).

По возможности не используйте один и тот же пароль для доступа к различным ресурсам внутри компании. Например, используйте один пароль для прикладных программ и другой для администрирования ресурсов. Используйте различные пароли для учётных записей Windows и Unix-систем.

2. Не сообщайте ваш пароль никому, даже вашему секретарю или обслуживающему персоналу. Все пароли являются конфиденциальной информацией *«ВАША КОМПАНИЯ»*.
3. Список запрещённых действий.
4. Не сообщайте никому свой пароль по телефону.
5. Не отправляйте свой пароль по электронной почте.
6. Не сообщайте свой пароль начальнику.
7. Не говорите о своём пароле рядом с посторонними.
8. Не упоминайте о содержимом пароля (например, «мой день рождения»).
9. Не указывайте свой пароль в анкетах или опросниках.
10. Не сообщайте свой пароль членам своей семьи.
11. Не сообщайте свой пароль сослуживцам перед уходом в отпуск.
12. Не записывайте пароль и не храните его на рабочем месте.
13. Не храните пароль в файле на компьютере, включая переносной, без шифрования.
14. Не используйте функцию «Запомнить пароль» в таких приложениях как Eudora, Outlook или Netscape Messenger

Если кто-либо требует сообщить ваш пароль, сошлитесь на этот документ или попросите позвонить в отдел информационной безопасности.

Если вы считаете, что учётная запись или пароль скомпрометированы, сообщите об этом в отдел информационной безопасности *«ВАША КОМПАНИЯ»* и смените все пароли.

Уполномоченные лица *«ВАША КОМПАНИЯ»* могут регулярно проводить подбор или попытки взлома паролей. Если пароль будет угадан или взломан во время таких мероприятий, вас попросят сменить пароль.

8. Стандарт разработки приложений. Разработчики приложений должны обеспечить в своих программах следующие меры безопасности:

1. Приложения должны поддерживать аутентификацию отдельных пользователей, а не групп.
2. Приложения не должны хранить пароли в открытом или легкораскрываемом виде.
3. Приложения должны обеспечивать своего рода передачу прав, чтобы один пользователь мог выполнять функции другого не зная его пароль.
4. Приложения должны по возможности всегда поддерживать TACACS+, RADIUS, и/или X.509 на основе LDAP.

9. Использование паролей и парольных фраз для удалённого доступа.

Для контроля удалённого доступа к сетям *«ВАША КОМПАНИЯ»* используйте или одноразовые пароли или ассиметричную ключевую систему со стойкой парольной фразой.

Парольные фразы отличаются от паролей. Парольная фраза более длинная версия пароля и, таким образом, более надёжная. Парольные фразы обычно используются для аутентификации в ассиметричных системах шифрования. Ассиметричная ключевая система определяет математическую связь между открытым ключом, известным всем и закрытым ключом, известным только его владельцу. Без парольной фразы, дающей доступ к закрытому ключу, пользователь не получит доступ.

Парольная фраза обычно состоит из нескольких слов, являясь более устойчивой к атакам по словарю. Хорошая парольная фраза относительно длинная и содержит комбинацию букв в верхнем и нижнем регистре, а

также цифры и знаки препинания. Вот пример хорошей парольной фразы: «The*?#>*@TrafficOnThe101Was*&#!#This Morning»

Все правила создания стойких паролей относятся и к парольным фразам.

10. Ответственность. Любой сотрудник, нарушивший настоящую политику, может быть подвергнут взысканию вплоть до увольнения.

Использование менеджеров паролей.

Необходимость использования менеджеров паролей связана непосредственно со сложностью запоминания многочисленных логинов и паролей для различных Web сайтов. Естественно, менеджеры паролей могут увеличить уровень безопасности, поскольку они позволяют использовать большое количество различных идентификаторов и паролей. Таким образом пользователь может сгенерировать много имен пользователей и, таким образом, усложнить процесс угадывания для атакующего. Ключевым моментом здесь является то, что пользователь должен доверять приложению выполнение его роли (безопасное хранение, обработка и перенаправление данных авторизованному узлу). Менеджеры паролей не являются панацеей, хотя они усиливают безопасность и повышают планку для атакующего путем использования интерфейса пользователя для обработки окружений, требующих аутентификацию.

Пользователи и компании должны быть уверены в том, что системы управления паролями корректно внедрены и корректно используются с учетом возможных факторов риска.

Использование одинаковых логинов и паролей на различных Web сайтах увеличивает вероятность компрометации, поскольку атакующему будет необходимо узнать только имя пользователя и пароль для получения доступа ко всем ресурсам пользователя.

Используя менеджер паролей, вам нужно запомнить только один пароль, так как менеджер паролей хранит и даже создает пароли для разных учетных записей, при необходимости автоматически входя в систему.

Смотрите на менеджера паролей, как на книгу ваших паролей, запертую ключом, который известен только вам. Некоторые подумают, что это плохо, потому что если кто-то завладеет этим ключом, то получит ВСЕ пароли. Но если вы выберете надежный и уникальный и при этом легко запоминающийся пароль, то получите практически идеальный способ защиты остальных ваших паролей от несанкционированного доступа.

Менеджеры паролей не только хранят ваши пароли, они помогают генерировать и сохранять надежные и уникальные пароли при регистрации на новых веб-сайтах. Это значит, что при обращении к веб-сайту или приложению вы можете открыть ваш менеджер паролей, скопировать пароль, вставить его в поле авторизации и получить доступ. Часто менеджеры паролей содержат расширения к браузеру, которые автоматически подставляют пароли за вас.

Многие используемые менеджеры паролей могут синхронизироваться между устройствами, применяя шифрование, поэтому ваши пароли доступны вам везде, даже на телефоне.

Менеджеры паролей предназначены для обеспечения доступа ко всем вашим паролям в зашифрованном виде, недоступном для хакеров и вредоносных программ. Они предлагают большое удобство и отличную защиту, гарантируя приватность ваших данных.

В целом, есть два типа менеджеров паролей:

- персональные менеджеры паролей, которые управляют паролями доступа к различным приложениям и услугам индивидуальных пользователей/сотрудников;

- менеджеры паролей от привилегированных учетных записей. Такие специализированные корпоративные решения защищают и управляют привилегированными учетными данными с помощью централизованного

корпоративного хранилища паролей. Привилегированные учетные данные являются наиболее защищаемыми секретами, обеспечивающими привилегированный доступ к учетным данным пользователей, приложениям, системам. Они часто идут в связке с системами управления сеансами привилегированного доступа и являются основным компонентом корпоративной платформы управления привилегиями.

Практическая часть.

На практической части этой работы мы изучим методы настройки менеджера паролей с помощью нашего браузера, а также с посредством специальных программ на примере ПО LastPass.

Менеджер паролей Google Chrome. Менеджер паролей в браузере обычно спрашивает вас, сохранять созданный пароль при первом входе на любом сайте. После этого менеджер паролей сохраняет его непосредственно в браузер и в зашифрованном виде загружает в ваш профиль на Google (если у вас включена синхронизация аккаунта).

Кроме того, менеджер паролей предложит вам сгенерировать надежный пароль при регистрации. Все пароли хранятся в зашифрованном виде, и вы можете управлять ими вручную. Чтобы увидеть сохраненные пароли, вам надо будет ввести администраторский пароль вашего компьютера или пароль для вашего аккаунта Google.

Чтобы открыть менеджер паролей Google Chrome, нажмите на значок своего профиля в верхнем правом углу окна браузера на компьютере (Рис №4.1).

Система менеджера подскажет, какие пароли надежные.

Менеджер паролей LastPass. LastPass – это инструмент управления паролями, к которому можно обратиться с любого компьютера, с любой точки земного шара, и в нужный момент получить доступ к сайтам с вашими данными. LastPass может генерировать пароли, и вам не нужно будет придумывать пароль для каждого сайта, он сам придумает.

Еще к плюсам LastPass можно отнести возможность работы с устройствами под управлением Windows, Linux, OS X, а также мобильные устройства Android, BlackBerry, WindowsMobile, Symbian, WebOS. В нем включена возможность автоматического заполнения форм, а также автоматическое нажатие войти. С ним вы сможете работать на любом браузере.

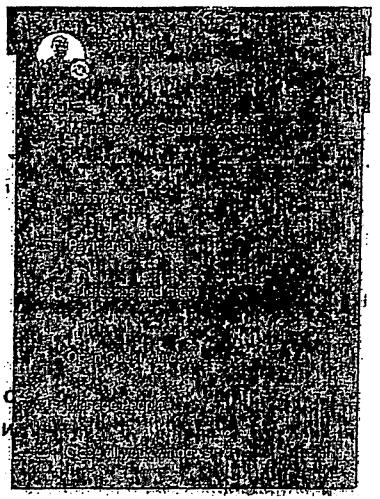


Рис. 4.1. Менеджер паролей Google Chrome.

В меню выберите "Пароли" (Рис. № 4.2.).

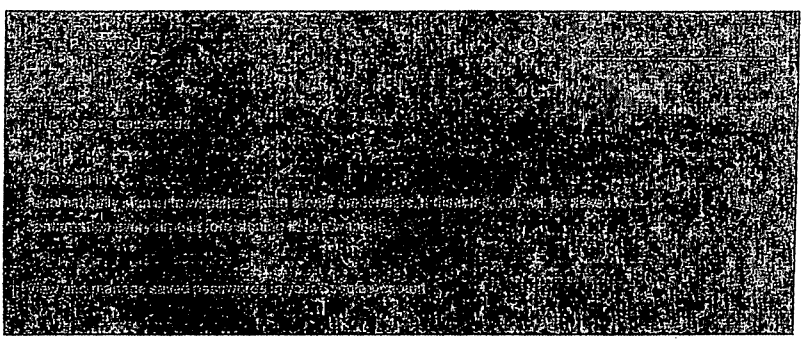


Рис.4.2. Оснастка «Пароли».

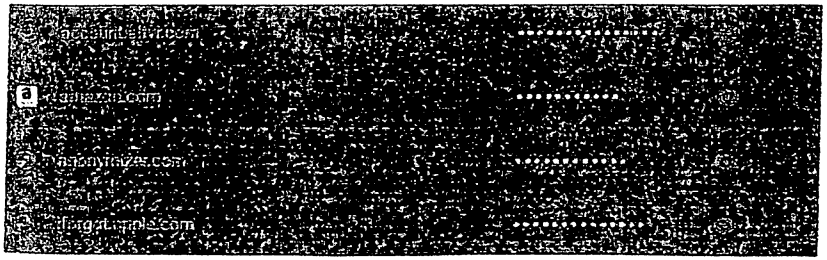


Рис. № 4.3. Список паролей от аккаунтов которые сохранены в менеджере.

Начнем с регистрации аккаунта LastPass и еще нужно загрузить программное обеспечение для компьютера.

1. Запускаем скачанный файл => выбираем язык и внизу нажимаем "дополнительные параметры" => или оставляем все по умолчанию, или добавляем нужные параметры и выбираем папку для установки (Рис.№4.4).

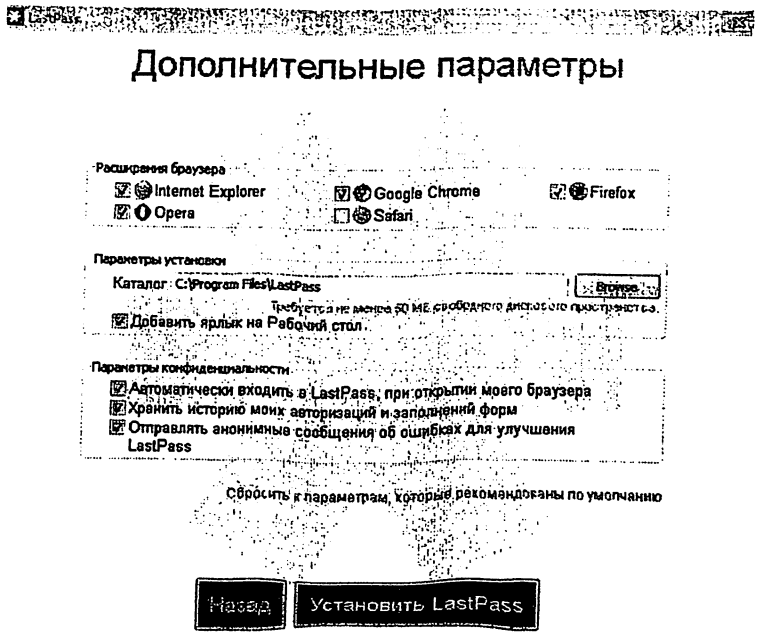


Рис. 4.4. Настройка дополнительных параметров.

2. На следующем этапе войти в существующую учетную запись или создать новую. Создавая новую учетную запись вам нужно придумать мастер-пароль, он должен быть надежным и лучше его не забывать. При вводе пароля надежность пароля снизу будет показывать на сколько он надежен, если вы не уверены в своей памяти – лучше запишите этот пароль (Рис №4.5.).

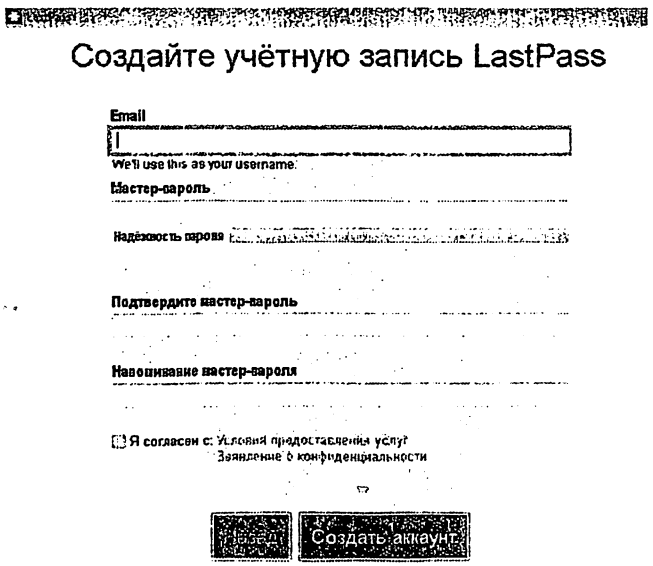


Рис. №4.5. Создание учетной записи LastPass.

3. После создания или входа – вам предложит импортировать пароли из браузеров, если вы не против – нажимаете "Импорт" (Рис.№4.6).

4. Вводим почту и пароль, ставим галочки если хотите, чтобы в этом браузере, и на данном компьютере вход выполнялся автоматически (Рис.№4.7.).

5. Теперь в каждом браузере (который вы выбрали в начале установки) появиться дополнение LastPass. Нажимаем на значок правой клавишей мыши, и выбираем параметры (Рис.№4.8.).

6. Здесь вы сможете настроить менеджер паролей на свой вкус: автоматический выход при закрытии браузера или истечении какого-то

времени, автоматическое заполнение полей, настройки различных уведомлений и подсказок, горячие клавиши и многое другое (Рис.№4.9).

Можно ничего не настраивать и всё оставить по умолчанию. После настройки можем приступать к работе.

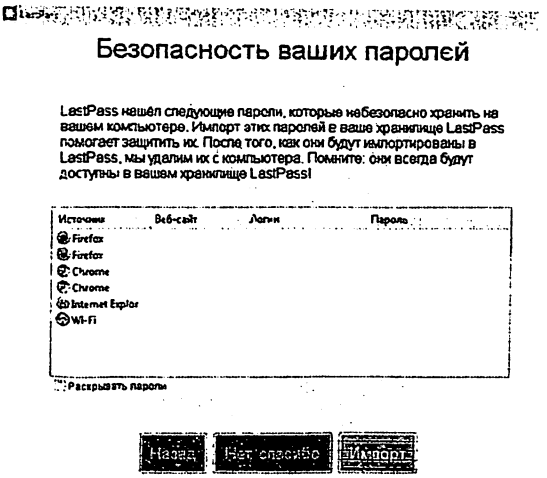


Рис.4.6. Импорт паролей с браузеров и приложений.

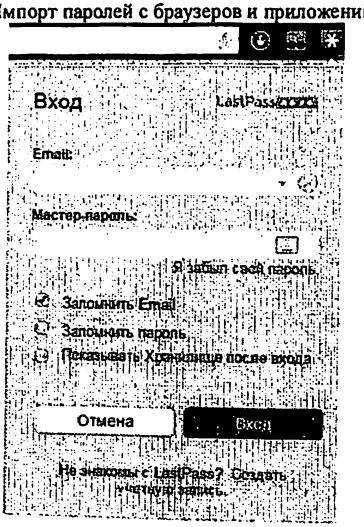


Рис. 4.7. Вход в систему.

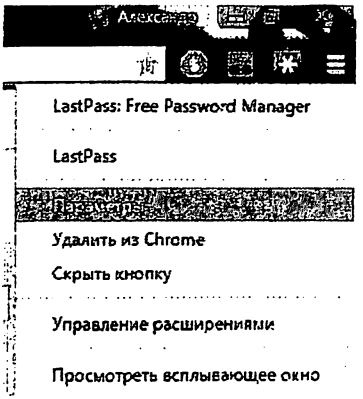


Рис. 4.8. Добавление LastPass в контекстное меню

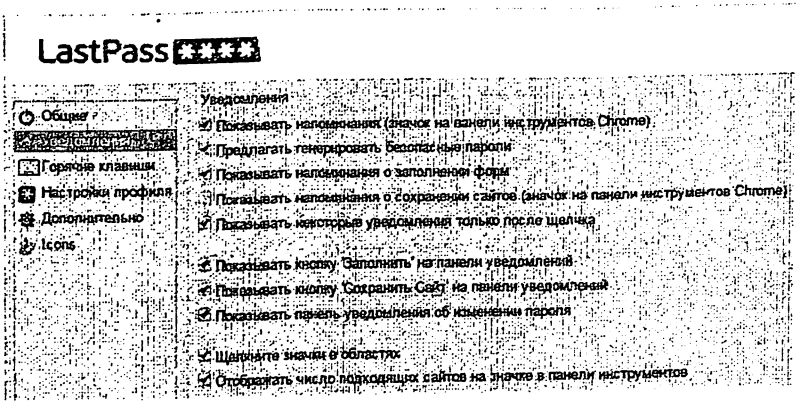


Рис.4.9. Настройка уведомлений.

Использование LastPass для генерирования и хранения безопасных паролей:

1. Во время регистрации на любом ресурсе LastPass будет предлагать создать защищенную учетную запись. К примеру, мы регистрируем почтовый ящик на mail.ru => заполняем поля и на поле где нужно придумать пароль нажимаем правой клавишей мыши, выбираем LastPass, и генератор безопасных паролей (Рис.№4.10).

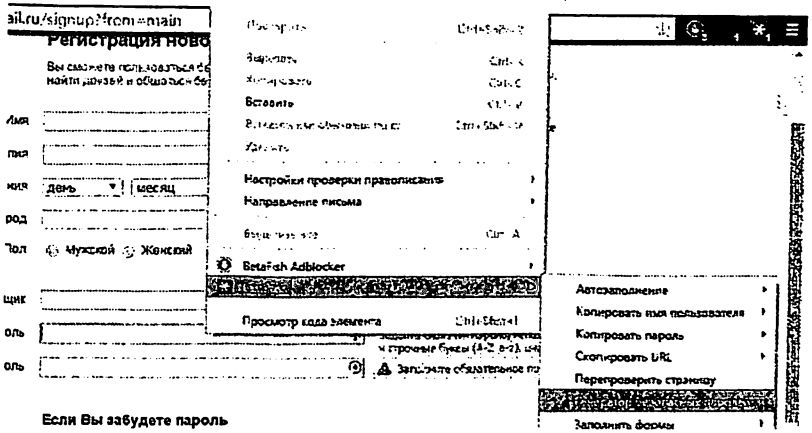


Рис.4.10. Использование генератора паролей LastPass.

2. В открывшемся окне вам предложит выбрать длину пароля, и сам пароль (Рис.№4.11.). Если пароль вам подходит – нажимаете принять, и он автоматически появляется в поле "пароль" и "подтверждения пароля", после регистрации LastPass будет помнить данный пароль для этой учетной записи.

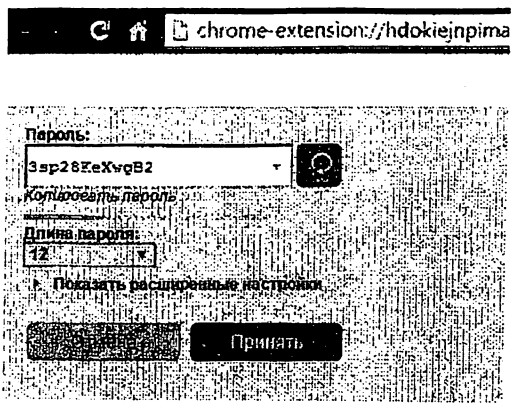


Рис.4.11. Генерация паролей.

3. Если вы входите на любой сайт под своей учетной записью – LastPass предлагает сохранить пароль или никогда не сохранять. Если вы сохраните

– дальше при каждом входе на сайт менеджер паролей будет предлагать авто заполнение, то есть автоматический вход (Рис.№4.12).

Рис.4.12. Предложение сохранения паролей на менеджере.

Задание:

Настроить менеджера паролей с помощью браузера, а также с посредством специальных программ на примере ПО LastPass и других программ.

Контрольные вопросы:

1. Что такое политика паролей и каково её цель?
2. Какие основные разделы включает в себя политика паролей?
3. Первый признак слабого пароля?
4. В чём заключается стойкость пароля?
5. В каких системах шифрования парольные фразы используются для аутентификации?
6. Какие типы менеджеров паролей вам известно и почему следует использовать их?

ПРАКТИЧЕСКАЯ РАБОТА №5. РЕЗЕРВНОЕ КОПИРОВАНИЕ ПОЛЬЗОВАТЕЛЬСКИХ ДАННЫХ С ПОМОЩЬЮ ОБЛАЧНЫХ СЕРВИСОВ.

Цель работы: Освоение практических навыков по формированию типичной политики резервного копирования и по настройке сервиса для резервного копирования и восстановления данных на примере Cloud Backup and Recovery (CBR).

Теоретическая часть.

О том, как трудно восстановить огромное количество важной информации, вы наверняка знаете, если хотя бы раз в жизни теряли важные

бумажные документы. К счастью, электронную информацию сохранить легче. Чтобы избежать ее случайного или преднамеренного удаления с компьютера, была придумана специальная процедура, которая позволяет дублировать все важные данные, – резервное копирование.

Ниже приведена «Типовой регламент резервного копирования данных». Типичная политика резервного копирования состоит следующих разделов:

1. Список терминов и определений.
2. Общие положения.
3. Порядок резервного копирования.
4. Контроль результатов резервного копирования.
5. Ротация носителей резервной копии.
6. Восстановление информации из резервных копий.

1. Список терминов и определений

- Заказчик – Компания _____
- Исполнитель – Компания _____.
- ГСА (группа системных администраторов) - группа сотрудников Исполнителя, обеспечивающая развитие и устранение сложных неисправностей ИТ-инфраструктуры Заказчика.
- ГТП (группа технической поддержки) – группа сотрудников Исполнителя, обеспечивающая техническую поддержку сотрудников Заказчика.
- ИТ-инфраструктура - совокупность аппаратного и программного обеспечения компании Заказчика, а также правил и методов их настройки, обеспечивающих технологию совместной работы сотрудников Заказчика.
- Администратор файлового сервера – сотрудник Исполнителя из числа ГСА, осуществляющий управление файловым сервером
- Сотрудник технической поддержки – сотрудник Исполнителя из числа ГСА.

- Заявка – запрос сотрудника предприятия к службе технической поддержки на решение какой-либо технической проблемы. Заявка содержит описание проблемы и электронный адрес сотрудника.
- Ресурс файлового сервера (далее Ресурс) – это каталог на файловом сервере, предназначенный для хранения файлов в целях, указанных в заявке на создание ресурса.
- Ответственный за информационные ресурсы Заказчика – сотрудник Заказчика из числа руководителей принимающий решения о создании новых Ресурсов.
- ИС «Helpdesk» – информационная система, обеспечивающая прием и обработку заявок сотрудников Заказчика.
- ИСМ – информационная система мониторинга ИТ-инфраструктуры Заказчика.
- ЭЦП – электронная цифровая подпись.
- GPG – программное обеспечение для шифрования и ЭЦП данных.
- Согласование Заявки – направление электронного сообщения (email) подтверждающего Заявку в ИС «Helpdesk» с ЭЦП. Для создания ЭЦП используется программное обеспечение PGP.
- Ответственный за ресурс – сотрудник Заказчика указанный ответственным в заявке на создание ресурса.

2. Общие положения

Настоящий Регламент проведения резервного копирования (восстановления) программ и данных, хранящихся на серверах ИТ-инфраструктуры Заказчика разработан с целью:

- определения порядка резервирования данных для последующего восстановления работоспособности автоматизированных систем Заказчика при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

- определения порядка восстановления информации в случае возникновения такой необходимости;
- упорядочения работы должностных лиц Исполнителя и Заказчика, связанной с резервным копированием и восстановлением информации.

В настоящем документе регламентируются действия при выполнении следующих мероприятий:

- резервное копирование;
- контроль резервного копирования;
- хранение резервных копий;
- полное или частичное восстановление данных и приложений.

Резервному копированию подлежит информация следующих основных категорий:

- персональная информация пользователей (личные каталоги на файловых серверах);
- групповая информация пользователей (общие каталоги отделов);
- информация, необходимая для восстановления серверов и систем управления базами данных (далее – СУБД);
- персональные профили пользователей сети;
- информация автоматизированных систем, в т.ч. баз данных;
- справочно-информационная информация систем общего использования («Гарант», «Консультант+» и т.п.);
- рабочие копии установочных компонент программного обеспечения рабочих станций;
- регистрационная информация системы информационной безопасности автоматизированных систем.

Машинным носителям информации, содержащим резервную копию, присваивается гриф конфиденциальности по наивысшему грифу содержащихся на них сведений в соответствии с «Перечнем сведений составляющих коммерческую тайну» Заказчика.

3. Порядок резервного копирования

Резервное копирование автоматизированных систем производится на основании следующих данных:

- состав и объем копируемых данных, периодичность проведения резервного копирования;
- максимальный срок хранения резервных копий - 1 месяц;
- хранение 3-х следующих архивов;
- архив на 1-е число текущего месяца;
- архив среда-четверг, либо пятница-суббота текущей недели;
- архив сделанный в текущую ночь.

Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, указанной в Перечне, в установленные сроки и с заданной периодичностью. Методика проведения резервного копирования описана в Приложении №3.

О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, сообщается в Службу безопасности Заказчика служебной запиской в течение рабочего дня после обнаружения указанного события. Ответственным является администратор резервного копирования.

4. Контроль результатов резервного копирования

Контроль результатов всех процедур резервного копирования осуществляется ответственными должностными лицами, в срок до 17 часов рабочего дня, следующего за установленной датой выполнения этих процедур.

В случае обнаружения ошибки лицо, ответственное за контроль результатов, сообщает в ГТП до 18 часов текущего рабочего дня.

На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с

использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для ее хранения.

5. Ротация носителей резервной копии

Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации автоматизированных систем в случае отказа любого из устройств резервного копирования. В случае необходимости замены испорченных носителей информации новыми, Исполнитель заблаговременно за 10 рабочих дней согласовывает с Заказчиком спецификации новых носителей информации.

Все процедуры по загрузке, выгрузке носителей из системы резервного копирования, а также перемещение их в Службу безопасности и обратно, осуществляются администратором резервного копирования по запросу и в присутствии ответственного сотрудника Службы безопасности Заказчика.

В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

Конфиденциальная информация с носителей, которые перестают использоваться в системе резервного копирования, должна стираться с использованием программного обеспечения PGP.

6. Восстановление информации из резервных копий

В случае необходимости восстановление данных из резервных копий производится на основании Заявки владельца информации, согласованной с Ответственным за информационные ресурсы Заказчика.

Процедура восстановления информации из резервной копии осуществляется в соответствии с методикой восстановления информации.

После поступления заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

Типичному регламенту резервного копирования прилагаются приложения, такие как:

1. Перечень резервируемой информации.
2. Перечень лиц ответственных за резервное копирование.
3. Методика резервного копирования.
4. Методика восстановления данных.

Практическая часть.

На практической части изучим как использовать **Cloud Backup and Recovery (CBR)** — сервис для резервного копирования и восстановления данных.

CBR позволяет выполнить резервное копирование облачных дисков и серверов. Это предотвращает потерю данных при вирусных атаках, случайных удалениях информации, а также при программном или аппаратном сбое.

Сервис включает в себя:

- резервные копии (*backups*) – обеспечивают сохранность данных серверов и дисков на основе технологии снимков (snapshots);
- хранилища (*vaults*) – CBR использует хранилища для агрегирования резервных копий;
- политику резервного копирования (*backup policies*) – применяется для выполнения автоматического копирования в определенные временные интервалы, также содержит правила хранения созданных копий.

Преимущества этого сервиса:

- Решение CBR поддерживает резервное копирование дисков в момент сбоя оборудования на облачный сервер, а также резервное копирование серверов баз данных в момент сбоя приложения, что обеспечивает безопасность и надежность ваших данных.

- Постоянные инкрементальные резервные копии сокращают время резервного копирования на 95%. Мгновенное восстановление с RTO в несколько минут.
- Настроить резервное копирование можно всего за три шага, а профессиональное владение ПО для резервного копирования не требуется. По сравнению с обычными системами резервного копирования, CBR использовать удобнее.
- Вы можете скопировать или восстановить данные резервной копии в любом регионе, что обеспечивает удаленное аварийное восстановление.

Этот сервис имеет ограничения и особенности:

- Одно хранилище может быть связано только с одной политикой резервного копирования.
- Максимальное количество связанных ресурсов — 256.
- Всего можно создать 32 политики резервного копирования.
- Для восстановления данных можно использовать только резервные копии в хранилище, состояние которых «Available» или «Locked».
- Резервные копии нельзя загрузить на локальный компьютер или в OBS (Object Storage Service — сервис хранения и управления объектным хранилищем данных).

Резервное копирование виртуальной машины (backup).

Резервное копирование может производиться вручную или автоматически.

При копировании вручную имя создаваемой копии будет вида manualbk_xxx. При автоматическом копировании имя создаваемой копии будет autobk_xxx.

По умолчанию, при создании первой копии ECS производится полное резервное копирование. При создании дальнейших копий, как автоматических, так и ручных, будут копироваться изменения с момента

последнего копирования. Воссоздание ECS возможно как с первой копии, так и с последующих.

Создание первой резервной копии состоит из нескольких этапов:

1. Создание хранилища (*vault*) (для копии сервера или для копии диска).
2. (*Опционально, если не были прикреплены серверы при создании хранилища*) Прикрепление серверов или дисков к хранилищу.
3. (*Опционально, если не была определена политика автоматического копирования*) создание и прикрепление политики резервного копирования к хранилищу.
4. (*Опционально, если требуется немедленное создание резервной копии*) Немедленное создание резервной копии сервера или диска.

Ниже приведена как настраивать политику резервного копирования с помощью сервиса CBR.

Политика резервного копирования (backup policy).

Политика резервного копирования (*Backup Policy*) — это свод правил для копирования данных, включающих в себя: имя политики, статус, время выполнения работ по резервному копированию, период копирования и правила хранения копий данных. Правила хранения определяют продолжительность хранения, количество сохраненных резервных копий и порядок удаления более ранних копий.

После прикрепления виртуальной машины ECS к Backup Policy резервное копирование будет осуществляться на регулярной основе в соответствии с правилами резервной политики.

Backup Policy необходима для автоматического создания резервных копий ECS в заданные временные интервалы.

Максимум можно создать 31 политику. К одной политике резервного копирования может быть прикреплено до 64 виртуальных машин ECS.

Можно воспользоваться политикой резервного копирования по умолчанию (defaultPolicy), которая позволяет выполнять ежедневный бэкап в 10.00.

Создание политики резервного копирования (Backup Policy)

1. Войдите в консоль управления.
2. В разделе Storage выберите пункт Cloud Backup and Recovery (*CBR*).
3. Перейдите в раздел Policies. Нажмите кнопку Create Policy.
4. В окне параметров политики укажите:

- Name — имя политики.
- Status — политику копирования можно использовать только когда она во включенном (рабочем) состоянии.
- Execution Time — можно добавить до 24 временных ячеек, но интервал между ними может превышать 1 час (Рис. №5.1)
- Backup Cycle — выберите периодичность копирования. Один из двух вариантов:

  A) Weekly-based Cycle — выберите дни недели создания копий (Рис.№5.2);

  B) Custom Cycle — можно указать временной интервал (Рис.№5.3), через какое количество дней должна создаваться резервная копия (выбор от 1 до 30 дней).

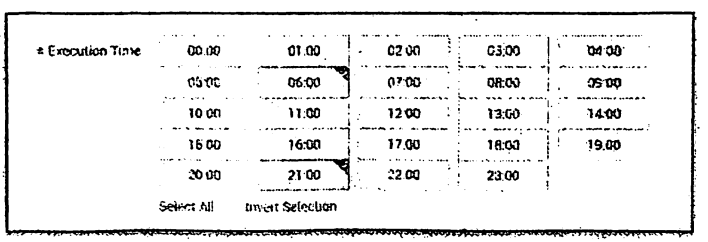


Рис. 5.1. Настройка Execution Time.

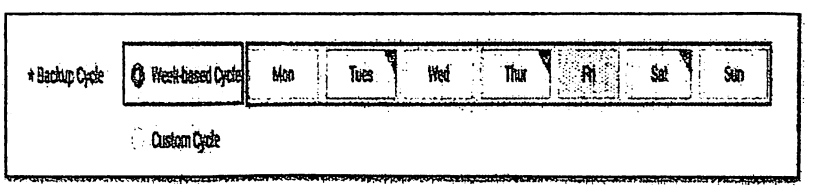


Рис. 5.2. Выбор периодичности копирования: Weekly-based Cycle.

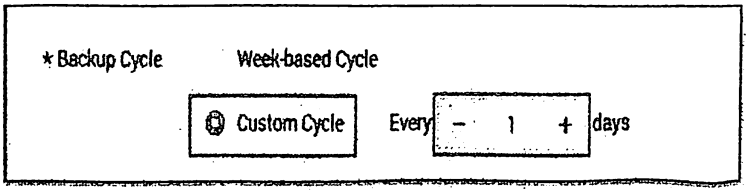


Рис. 5.3. Выбор периодичности копирования: Custom Cycle.

- Retention Rule — правило хранения резервных копий — определяет, как долго будут храниться созданные копии. Выберите один из трех вариантов и нажмите ОК:

  A) Backup Quantity — укажите количество сохраняемых копий. При превышении указанного числа наиболее ранняя из копий удаляется (при нажатии Long-term retention settings можно настроить количество сохраненных копий в день, неделю, месяц и год (будут сохранены самые ранние копии за указанный период));

  B) Time Period — через какой период времени копия должна удаляться (Рис.№5.4.). Можно указать с точностью до дня (пункт Custom в раскрывающемся списке);

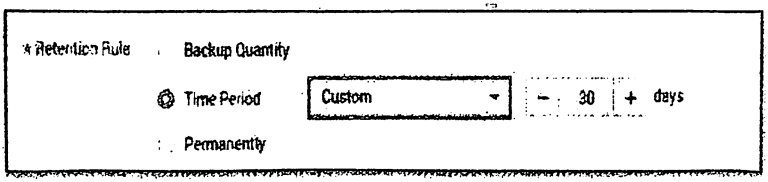


Рис.5.4. Настройка опции Time Period

  C) Permanently — при выборе этой опции автоматического удаления копий не будет (Рис.№5.5.).

- В конце проделенных настроек нажмите «Submit».

Назначение политики копирования серверам.

1. В сервисе Cloud Backup and Recovery перейдите во вкладку Cloud Server Backup.

2. В строке с хранилищем, к которому нужно прикрепить политику резервного копирования, нажмите More и выберите Set Backup Policy.
3. В поле Backup Policy выберите нужную политику и нажмите OK.

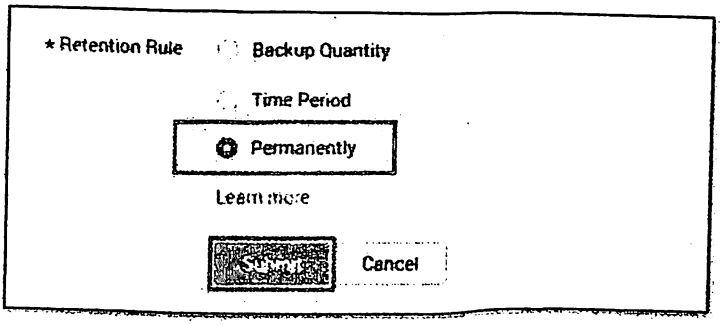


Рис.5.5. Выбор опции Permanently и завершение работы.

Назначение политики копирования дискам.

1. В сервисе Cloud Backup and Recovery перейдите во вкладку Disk Backup.
2. В строке с хранилищем, к которому нужно прикрепить политику резервного копирования, нажмите More и выберите Set Backup Policy.
3. В поле Backup Policy выберите нужную политику и нажмите OK.

Открепление политики копирования.

Для отмены автоматического бэкапа у хранилища нужно открепить политику резервного копирования. Это можно сделать через хранилище, к которому политика прикреплена.

Также можно деактивировать статус политики через хранилище или через раздел Policies. При этом политика перестанет работать у всех хранилищ, к которым она прикреплена.

1. В сервисе Cloud Backup and Recovery перейдите во вкладку Cloud Server Backup (или Disk Backup).
2. На вкладке Vaults нажмите на имя нужного хранилища.
3. В блоке «Policies» нажмите «Unbind Policy». Затем нажмите «Yes».

Изменение политики резервного копирования.

1. В сервисе Cloud Backup and Recovery перейдите во вкладку Policies.
2. В строке с нужной политикой нажмите Edit.
3. Сделайте необходимые изменения и нажмите Submit.

Отключение Backup Policy.

Для отключения автоматического копирования у всех серверов и дисков, к хранилищам которых прикреплена конкретная политика, следует отключить саму политику резервного копирования.

1. В сервисе Cloud Backup and Recovery перейдите в раздел Policies.
2. В строке с политикой, которую нужно отключить, нажмите Disable Backup Policy.
3. Нажмите Yes.

Включение Backup Policy.

После включения политики автоматическое копирование будет включено у всех серверов и дисков, к хранилищам которых данная политика прикреплена.

1. В сервисе Cloud Backup and Recovery перейдите в раздел Policies.
2. В строке с политикой, которую нужно отключить, нажмите Enable Backup Policy.
3. Нажмите Yes.

Удаление политики резервного копирования.

1. В сервисе Cloud Backup and Recovery перейдите во вкладку Policies.
2. В строке с нужной политикой нажмите Delete.
3. Нажмите Yes.

Задание:

1. Настроить резервное копирование и восстановление данных на примере Cloud Backup and Recovery (CBR) и других подобных программ.
2. Настроить основные параметры такие, как «Создание политики резервного копирования», «Выбор периодичности копирования», «Назначение политики копирования серверам», «Назначение

политики копирования дискам», «Отключение Backup Policy», «Удаление политики резервного копирования».

Контрольные вопросы:

1. Резервное копирование это? Виды резервных копий.
2. Какими рисками обусловлены создание резервных копий?
3. Периодичность (частота) резервного копирования?
4. На какие параметры нужно обращать внимание при создании резервных копий системы?
5. Какие приложения прилагаются к типичному регламенту резервного копирования?
6. Из каких разделов состоит Типичная политика резервного копирования?
7. На основании каких данных производится резервное копирование автоматизированных систем?

ПРАКТИЧЕСКАЯ РАБОТА №6.
СРЕДСТВА ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ПОЛЬЗОВАТЕЛЬСКИХ ДАННЫХ В СЕТИ ИНТЕРНЕТ.

Цель работы: Приобретение практических навыков по применению политики безопасности в защите персональных данных и настройке средств обеспечения конфиденциальности пользовательских данных в сети Интернет на примере ПО TOR.

Теоретическая часть.

Сбор, систематизация и хранение персональных данных граждан Узбекистана при их обработке должны осуществляться на технических средствах, физически размещенных в Узбекистане. Дополнение об этом внесено в закон о персональных данных.

Президент Узбекистана Шавкат Мирзиёев 14 января подписал закон, которым внесено дополнение в закон «О персональных данных». Закон

«О персональных данных» был принят в июле 2019 года и вступил в силу с 1 октября того же года.

Документ дополнен статьёй 27–1 «Особые условия обработки персональных данных граждан Республики Узбекистан. Она гласит:

«Собственник и (или) оператор при обработке персональных данных граждан Республики Узбекистан с использованием информационных технологий, в том числе во всемирной информационной сети Интернет, обязан обеспечить их сбор, систематизацию и хранение в базах персональных данных на технических средствах, физически размещенных на территории Республики Узбекистан и зарегистрированных в установленном порядке в Государственном реестре баз персональных данных».

Под персональными данными понимается «зафиксированная на электронном, бумажном и (или) ином материальном носителе информация, относящаяся к определенному физическому лицу или дающая возможность его идентификации».

Правильное построение политики безопасности играет важную роль в защите конфиденциальных данных.

Успех политики безопасности больше зависит от усилий и опытности людей, реализующих политику, чем от сложных технических средств контроля.

Независимо от типа политики организации в области допустимого использования Интернета главным фактором, влияющим на поведение пользователей, является их обучение. Пользователи должны быть знать, что они являются составной частью репутации организации и использование ими Интернета влияет на репутацию. Пользователи должны знать, что каждое посещение ими сайтов Интернета оставляет на них следы, и знать, почему организация оставляет за собой право наблюдать за использованием Интернета. Администраторы должны знать о своих обязанностях в отношении используемых программно-аппаратных средств (например, для

блокирования доступа к сайтам, наблюдения за работой) для реализации принятой в организации политики.

Политика использования Интернета - низкий риск. Интернет считается важной ценностью организации. Пользователям рекомендуется использовать Интернет и учиться делать это профессионально. С помощью такого открытого доступа сотрудники должны лучше выполнять свои обязанности.

Сотрудники не должны использовать Интернет для своих личных целей, и не должны посещать вредные и порнографические сайты, а также не должны получать доступ или использовать информацию, которая считается оскорбительной. Деятельность сотрудников, нарушающих это, будет контролироваться и они будут наказаны, вплоть до уголовного наказания.

Доступ к Интернету с компьютера, принадлежащего организации или через соединение, принадлежащее организации, должен соответствовать требованиям политик, касающихся допустимого использования техники организации. Сотрудники не должны позволять членам своих семей или посторонним лицам получать доступ к компьютерам организации.

Пользователи, посылающие письма в группы новостей USENET и списки рассылки, должны включать пункт о том, что это их личное мнение, в каждое сообщение.

Невозможно составить список всех возможных видов неавторизованного использования, поэтому дисциплинарные наказания применяются только после того, как другие способы исчерпали себя. Примерами неприемлемого использования, которое приводит к наказаниям, являются:

- неавторизованные попытки получить доступ к компьютеру
- использование рабочего времени и ресурсов организации для личной выгоды
- кража или копирование файлов без разрешения

- посылка конфиденциальных файлов организации во внешние компьютеры или в другие внутренние компьютеры неавторизованными на это людьми
- отказ помогать сотрудникам отдела информационной безопасности
- посылка писем-пирамид по электронной почте

Политика использования Интернета - средний риск. Компьютеры и сети организации могут использоваться только для выполнения служебных обязанностей. Допускается редкое их использование в личных целях. Любое их использование, которое можно считать незаконным или нарушающим политику организации, или такое использование, которое наносит вред организации, может явиться причиной административных наказаний, включая увольнение. Все сотрудники должны бережно использовать свои компьютеры.

Другой подход может быть таким:

Сетевое оборудование организации, включая сервера, доступные из Интернета, а также подключенные к ним компьютеры и установленные на них программы могут использоваться только для разрешенных целей. Начальники подразделений могут разрешить иногда иной доступ, если он не мешает выполнять служебные обязанности, не является слишком продолжительным и частым, служит интересам организации, таким как повышение квалификации ее сотрудников, и не приводит к дополнительным расходам для организации.

Письма пользователей в группы новостей USENET, списки рассылки и т.д. должны включать строку о том, что точка зрения, выраженная в письме - личная точка зрения, а не точка зрения организации.

Личные бюджеты пользователей онлайновых сервисов не должны использоваться с компьютеров организации. Для получения доступа к платным сервисам с компьютера организации, она должна предварительно осуществить подписку на них и заплатить за это деньги.

Пользователям выдаются пароли для работы на компьютерах организации, чтобы защитить критическую информацию и сообщения от неавторизованного использования или просмотра. Такие пароли не защищают от просмотра информации руководством организации. Руководство оставляет за собой право периодически контролировать использование сотрудниками компьютерных систем и сетей.

Начальники подразделений отвечают за обеспечение гарантий того, что их подчиненные понимают политику допустимого использования Интернета.

Доступ к Интернету с домашнего компьютера должен соответствовать требованиям политик, касающихся допустимого использования техники организации. Сотрудники не должны позволять членам своих семей или посторонним лицам получать доступ к компьютерам организации.

Политика использования Интернета - высокий риск. Организация полностью соединена с Интернетом и другими сетями. В целом, пользователи имеют неограниченный доступ к сети. Но доступ из Интернета или других сетей к ресурсам организации разрешен только тогда, когда это требуется для выполнения служебных обязанностей.

Для личного использования Интернета сотрудниками имеется отдельный сервер доступа. Этот сервис должен использоваться только для отдельных сотрудников с обоснованием доступа к нему. С его помощью можно получать доступ только с тем сайтам, которые одобрены организацией.

Любое их использование, которое можно считать незаконным или нарушающим политику организации, или такое использование, которое наносит вред организации, может явиться причиной административных наказаний, включая увольнение. Все сотрудники должны бережно использовать свои компьютеры.

Письма пользователей в группы новостей USENET, списки рассылки и т.д. должны включать строку о том, что точка зрения, выраженная в письме - личная точка зрения, а не точка зрения организации.

Руководство оставляет за собой право периодически контролировать использование сотрудниками компьютерных систем и сетей

Доступ к Интернету с домашнего компьютера должен соответствовать требованиям политик, касающихся допустимого использования техники организации. Сотрудники не должны позволять членам своих семей или посторонним лицам получать доступ к компьютерам организации.

Сохранение конфиденциальности личной информации (privacy)

Политика конфиденциальности личной информации при использовании Интернета должна быть согласована с политиками конфиденциальности личной информации в других областях. Хотя технически довольно просто наблюдать за сотрудниками, это плохая идея. На безопасность очень большое влияние оказывает мораль сотрудников. Сотрудники должны знать, что протоколы их работы на компьютерах могут быть сообщены посторонним организациям, таким как правительственные агентства, или по запросу согласно акту о свободе информации.

Низкий и средний риск. Соединение с Интернетом - это ресурс организации. Деятельность сотрудников организации в Интернете может наблюдаться, протоколироваться и периодически проверяться для того, чтобы организация имела гарантии того, сотрудники работают правильно, и могла защититься от неавторизованного использования Интернета. Кроме того, организация может получить доступ к любой информации пользователей или к любому взаимодействию пользователей. Организация может разгласить информацию, полученную таким образом уполномоченным на это третьим лицам, включая правоохранительные органы или запросы FOIA. Использование (список ресурсов) означает

согласие пользователя с тем, что за его деятельностью осуществляется контроль.

Обучение пользователей

Большинство компьютерных пользователей организации попадает в одну из трех категорий - интернет-мастера; пользователи, обладающие знаниями, но не обладающие опытом; пользователи, которые знают Интернет, провели в нем много времени, но не знают, как он устроен.

Большинство пользователей знает, что с использованием Интернета связан риск, но не понимает, с чем он связан, и как его избежать. Они часто не умеют распознать проблему с безопасностью, или как обезопасить себя при повседневном использовании Интернета. Они не знают последствий недопустимого или неавторизованного использования Интернета.

Доведите до пользователей их обязанности в области безопасности, и научите их, как надо себя вести - это изменит их поведение. Пользователи не могут соблюдать политики, которые они не понимают. Обучение также способствует индивидуальной отчетности, которая является самым важным способом повышения компьютерной безопасности. Не зная необходимых мер безопасности и как их применять, пользователи не смогут до конца отвечать за свои действия. Обучение также необходимо сетевым администраторам, которым требуются специальные навыки для понимания и реализации технологий, требуемых для обеспечения безопасности соединения с Интернетом. Риски, связанные с Интернетом, должны быть доведены до руководства организацией, чтобы обеспечить его поддержку.

Все пользователи, администраторы и руководители подразделений, имеющие доступ к Интернету, должны пройти начальный инструктаж в области безопасности и периодически проходить его снова. Обучение опытных пользователей должно быть, в основном, сосредоточено на вопросе допустимого использования Интернета. Например, почему организация приняла решение запретить прием определенных групп новостей USENET. Почему личные письма, в заголовке которых указан

почтовый домен организации, отражаются на репутации, независимо от того, использовалась фраза о том, что точка зрения, выраженная в письме - это личное мнение или нет. Некоторые пользователи, окончившие университет, могут испытать шок при доведении до них таких требований. Должен быть сделан упор на ролях и их ответственности, помимо технических проблем безопасности.

Пользователи, которые уже что-то знают, должны обучаться способам использования Интернета. Они могут быть достаточно хорошо знакомы с BBS, и должны быть проинформированы, что их письма будут теперь распространяться по всему миру, а не только в США или среди небольшой группы пользователей. Эти пользователи должны быть осмотрительны - перед тем, как написать письмо, следует сначала посмотреть, о чем пишут в данной группе новостей. Они не должны загружать программы или подписываться на информацию, пока не будут понимать последствий своих поступков - они могут подвергнуть организацию риску. А других пользователей, которые более продвинуты, чем остальные, надо учить, как стать более опытным пользователем Интернета, помимо обучения допустимому использованию Интернета, ответственности при работе в нем и технических вопросов безопасности.

Неграмотным же пользователям требуется объяснять все. Они должны узнать, что такое Интернет, какие виды сервисов он предоставляет, кто является его пользователями, и как установить с ним соединение. Они должны узнать о группах новостей и списках рассылки в Интернете, поисковых системах и этике в Интернете. Кроме того, они должны узнать все то, что изучают более грамотные пользователи.

Обучение безопасности в Интернете - низкий риск. Организация должна проводить периодическое обучение в области безопасности всех руководителей, операторов и конечных пользователей так, как это описано в политике организации. Такое обучение должно дополняться доведением новых проблем с безопасностью, постоянно возникающих в Интернете.

Пользователям рекомендуется просматривать списки рассылки, связанные с безопасностью, чтобы быть в курсе всех проблем и технологий и знать все новости, сообщаемые отделом информационной безопасности.

Обучение безопасности в Интернете - средний риск. В организации должна быть достаточно либеральная политика в отношении использования Интернета, но опытные пользователи должны повышать свой уровень в отношении эффективного использования Интернета и рисков, связанных с ним. Следует добавить приведенные ниже положения к тем, что указаны для организации с низким риском.

Обучение безопасности в Интернете должно включать проведение как комплексных, так и индивидуальных занятий со специалистами центров по обучению безопасности, краткое доведение информации о новостях и советов по использованию, а также другое необходимое обучение, как это принято в организации. . При обучении обязательно должны быть изучены следующие вопросы - использование брандмауэров, загрузка информации и программ, проблемы, связанные с апплетами, электронной почтой, списками рассылки, домашними страницами, браузерами, шифрование.

Администраторы брандмауэра и ЛВС, а также технический персонал сетей, подключенных к Интернету, должны пройти курс обучения в области контроля за безопасностью в сети, достоинств и недостатков различных подходов, возможных видов атак, сетевой архитектуры и вопросов, связанных с политикой безопасности.

Системные и сетевые администраторы должны пройти полный курс обучения в области администрирования брандмауэров.

Некоторые средства сканирования (например, pingall, SATAN) стали обязательным элементом при проведении контроля защищенности сети для выявления активных систем, их IP-адресов, параметров конфигурации и т.д. Кроме того, для выявления уязвимых мест в системах крайне полезны как бесплатные, так и коммерческие средства (например, SATAN, ISS, NETProbe, PINGWARE, COPS, Tripwire и др.). Все сетевые и системные

администраторы должны уметь их использовать. Они также должны знать текущее состояние дел в этой области безопасности.

Новые пользователи должны пройти вводный курс обучения работе в Интернете, который включает серьезную отработку практических навыков и обзор проблем безопасности. Все пользователи должны расписаться в журнале проведения инструктажей по использованию Интернета.

Обучение безопасности в Интернете - высокий риск. Организация должна стремиться повысить доступность Интернета для своих сотрудников, но делать это консервативным методом и только после обучения пользователей в области правил безопасности при использовании Интернета. Уместна следующая политика помимо политики, указанной для организации со средним риском.

Пользователи должны быть постоянно информированы о текущих проблемах с безопасностью в Интернете путем чтения сообщений и предупреждений об ошибках в программах и уязвимых местах и других советах, разборах имевших место происшествий, а также пройти курс обучения таким образом, как это определено в организации. При обучении обязательно должны быть изучены следующие вопросы - использование брандмауэров, загрузка информации и программ, проблемы, связанные с апплетами, электронной почтой, списками рассылки, домашними страницами, браузерами, шифрование.

Практическая часть.

Чтобы работать в сети анонимно существует множество решений такие как – the Onion router (TOR). Эта программа поможет вас защитить от наблюдения за вами в Интернете при помощи анализа потока данных, т.е., при использовании этого приложения никто, кроме вас, ни сможет узнать, кто вы, где вы находитесь и что посещаете в Интернете.

В этой практической работе рассматриваются основные моменты работы данной технологии, ее настройка и интеграция в браузер.

TOR (луковый роутинг) представляет из себя сеть виртуальных тоннелей, при помощи которых отдельные лица или группы людей могут улучшить свою приватность и безопасность пребывания в сети. При помощи этой технологии пользователи могут быть анонимными при «серфинге» веб-сайтов, размещении различных материалов, отправке электронных сообщений и в работе с приложениями, требующими доступа в интернет. Данная технология может обеспечить защиту от механизма анализа трафика, который грозит не только анонимности пользователя, а и его конфиденциальности бизнес данных, сохранения деловых контактов и других важных сведений.

Анонимность пользователя обеспечивается при помощи распределенной сети серверов, которые называются многослойными маршрутизаторами. Пользователь, запустивший TOR на своем компьютере, подключается к серверам TOR и периодически создает цепочку через сеть TOR, которая применяет криптографию многоуровневым способом. Каждый пакет данных вначале шифруется тремя ключами и проходит через три разных прокси-сервера (Рис №7.1.).

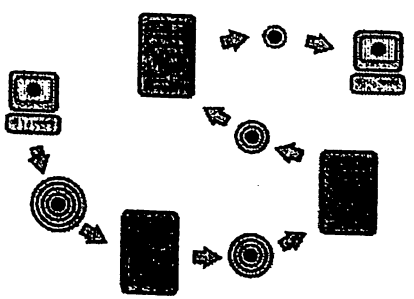


Рис 7.1. Работа технологии TOR

Возможности TOR:

- Посещение сайтов, заблокированные провайдером или системным администратором.

- работать через прокси-сервер.
- Запускать заблокированный трафик для IM (ICQ, Mailru-агент, джоббер и д.р.)
- TOR не нужно устанавливать. Поэтому не стоит бояться запрета на установку программ, выставленную вашим системным администратором.

Установка и настройка TOR

TOR, как и любое другое приложение лучше скачать с официального сайта – torproject.org. Заходим на сайт, находим картинку с надписью – Download Tor и жмем по ней (Рис. №7.2.).

Рис 7.2. Кнопка для скачивания TOR

На странице, которая откроется, в правом нижнем углу выбираем нужный вам язык меню программы (Рис №7.3.).

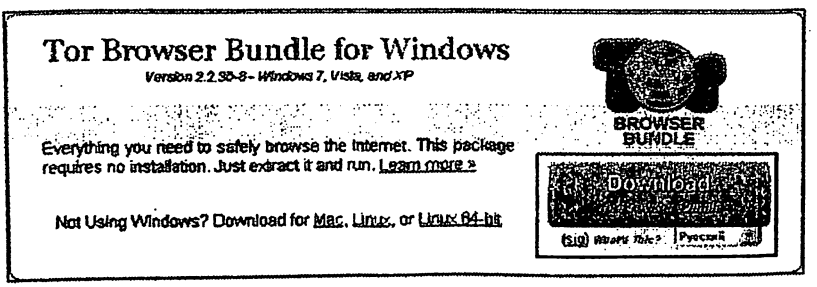


Рис 7.3. Выбор языка

Программа представляет из себя самораспаковывающийся архив. Поэтому при установке, ему нужно указать путь, куда распаковаться (Рис №7.4.).

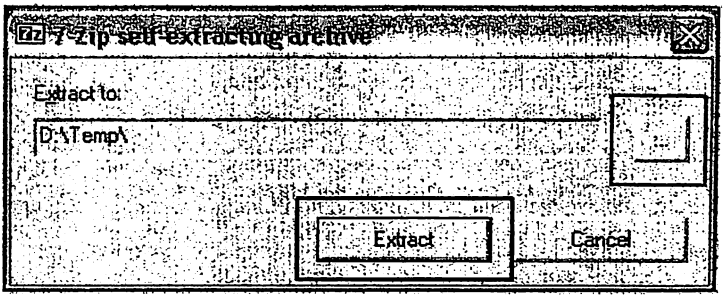


Рис 7.4. Выбор места распаковки

Нажимаем кнопку выбора папки для распаковки (обведена красным прямоугольником на картинке выше) и выбираем нужное вам место.

Т.к. программа не требует установки то ее можно распаковать на любой носитель информации и в дальнейшем производить запуск с любого компьютера.

Выбрав нужный каталог, жмем кнопку – Extract. Ждем какое-то время, пока архив распакуется (Рис №7.5.).

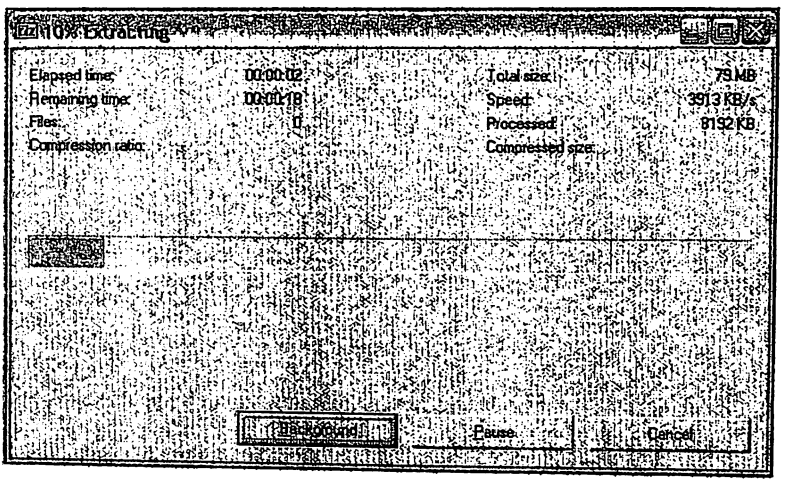


Рис 7.5. Распаковка приложения

По завершению распаковки в выбранном вами месте должна появиться папка – Tor Browser (Рис №7.6.).

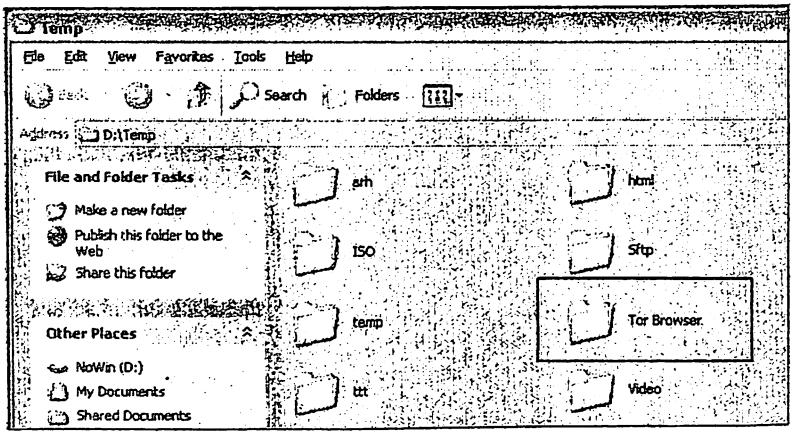


Рис 7.6. Папка – Tor Browser

Внутри этой паки находится файл – Start Tor Browser. Он и используется для запуска программы (Рис №7.7).

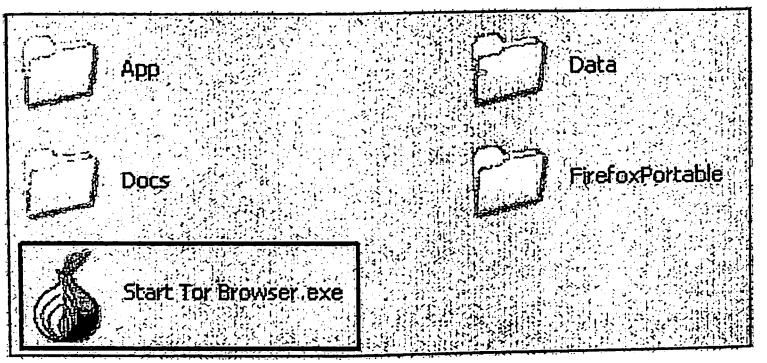


Рис 7.7. Файл запуска программы

Чтобы запустить программу нужно дважды кликать на программе – Start Tor Browser. Ждем пока программа будет выполнять нужные ей действия (Рис №7.8.).

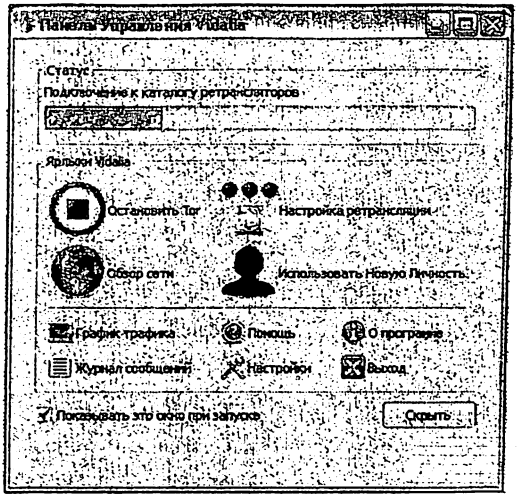


Рис 7.8. Процесс запуска программы

Первый запуск программы происходит довольно таки долго. После окончания запуска должно появиться меню как на картинке ниже (Рис №7.9.).

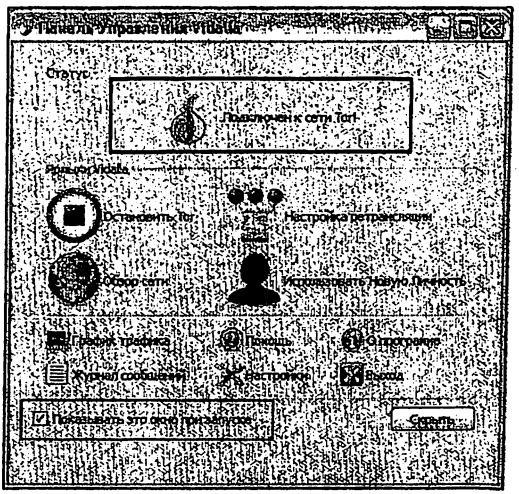


Рис 7.9. Меню программы

Надпись обведенная синей рамкой говорит о том, что приложение заработало. Для удобства можно снять галочку с пункта – Показывать это окно при запуске (обведена красным прямоугольником), т.к. после начала своей работы приложение будет запускать браузер – Mozilla Firefox (он идет совместно с программой) (Рис №7.10.).

Рис 7.10. Работа Mozilla Firefox

Теперь при запуске, программа будет находиться в трее и будет иметь три значения:

«Желтая луковица» – приложение запускается.

«Зеленая луковица» – приложение работает.

«Зачеркнутая луковица» – приложение остановлено.

Браузер – Mozilla Firefox должен показывать окно как на картинке ниже.

Если вы видите у себя такое окно, значит TOR работает. Но его действие будет распространяться лишь на браузер – Mozilla Firefox. И если его закрыть, то и TOR завершит свое действие. Поэтому, Mozilla можно свернуть в трей и настроить другой браузер на работу с TOR.

Настройка браузера Opera для работы с TOR

Для того чтобы понять работает ли TOR на вашем браузере, следует перейти по ссылке – https://check.torproject.org/?lang=ru. Вот что должна показать Opera (Рис №7.11.).

Чтобы заставить Opera работать с TOR, зайдите в ее настройки (Рис №7.12.). Для этого нажимаем кнопочку – Opera (обведена синим прямоугольником, картинка выше), в выпадающем меню выбираем пункт – Настройки (обведен красным прямоугольником), а в нем – Общие настройки (обведен зеленым прямоугольником). Также можно нажать сочетание клавиш – Ctrl + F12. Попадаем в настройки Opera (Рис №7.13).

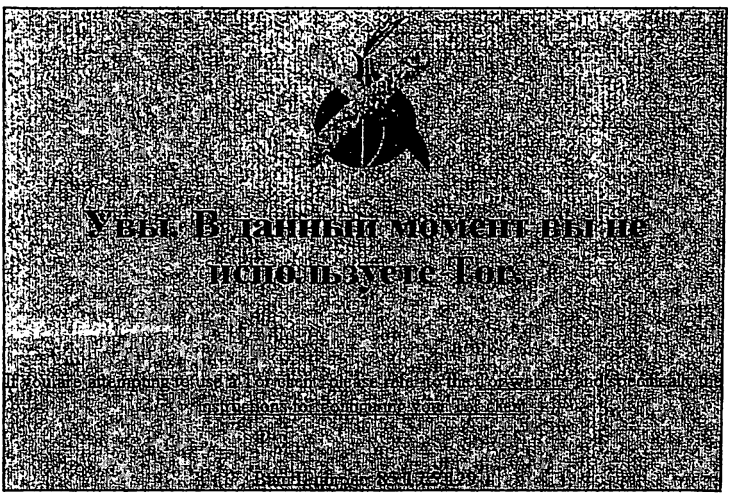


Рис 7.11. Сообщение браузера Opera

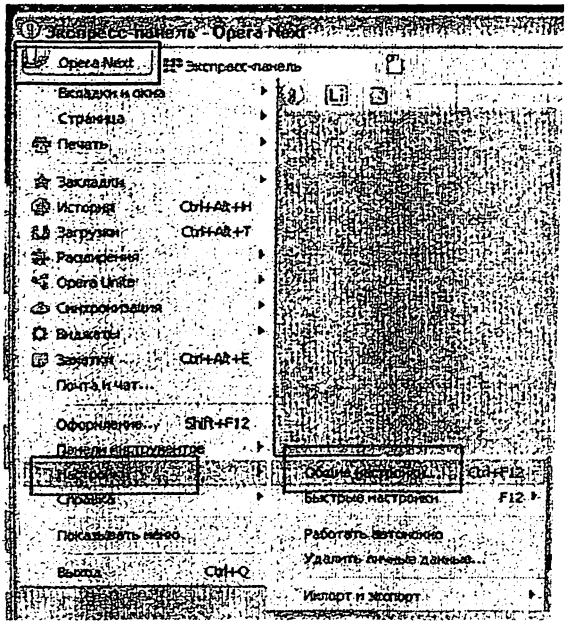


Рис 7.12. Настройка Opera

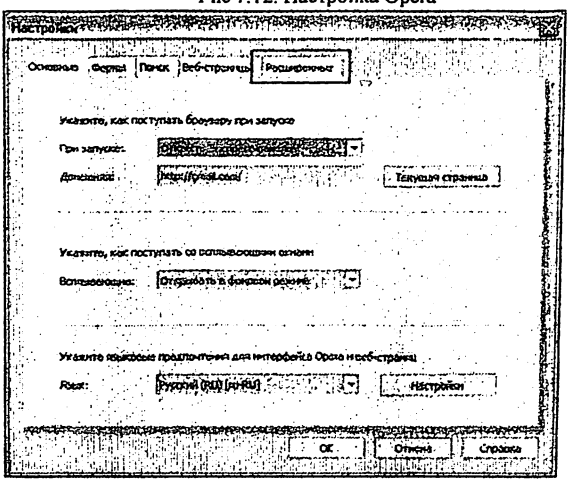


Рис 7.13. Меню настроек Opera

Здесь выбираем вкладку – Расширенные, затем пункт – Сеть. В меню – Сеть, жмем кнопку – Прокси-серверы. В появившемся окне заполняем все, как показано на картинке ниже (Рис №7.14).

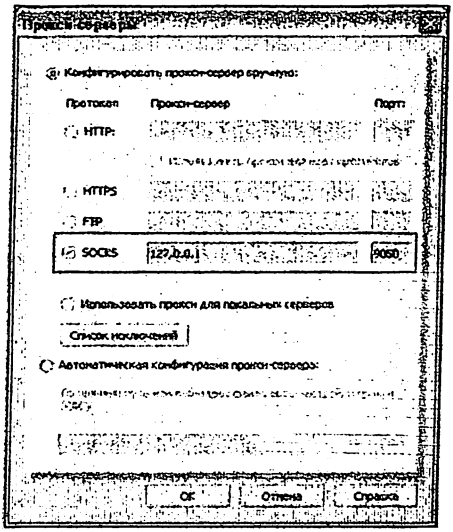


Рис 7.14. Меню – Прокси-серверы

Заполнив необходимые поля, жмем – Ок и перезагружаем браузер.

Производим проверку браузера на работу с TOR (переходим по ссылке, указанной выше). Должна быть такая картинка (Рис №7.15).

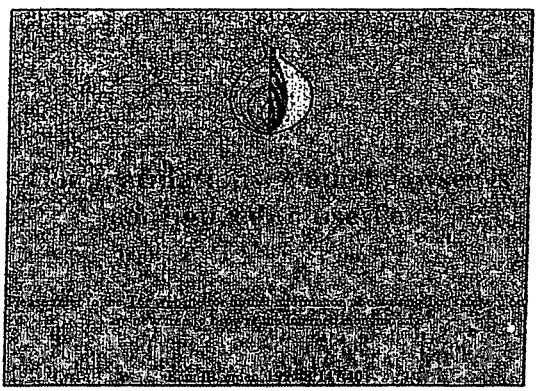


Рис 7.15. Работа Opera

Все, теперь работать в сети можно анонимно. Учитывайте, лишь, то, что скорость работы будет не слишком высокой, т.к. ваши запросы будут идти не по прямому пути, а через сервера TOR.

Задание:

Настроит средства обеспечения обеспечения конфиденциальности пользовательских данных в сети Интернет на примере ПО TOR

Контрольные вопросы:

1. Какие требования предъявляются к обработке персональных данных?
2. В каких ситуациях выдается доступ новому сотруднику в должности системных и сетевых администраторов?
3. Какой фактор является главным фактором, влияющим на поведение пользователей независимо от типа политики организации в области допустимого использования Интернета?
4. При обучении сотрудников какие основные темы должны быть изучены?

ПРАКТИЧЕСКАЯ РАБОТА №7.
МЕРЫ ПО ЗАЩИТЕ ОТ УГРОЗ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ (ОГРАНИЧЕНИЕ СПАМА В ПОЧТЕ, КОНТРОЛЬ ССЫЛОК).

Цель работы: Освоение практических навыков по использованию средств по защите от угроз социальной инженерии (ограничение спама в почте, контроль ссылок)

Теоретическая часть.

Термин «социальная инженерия» обозначает способ получения злоумышленником нужной информации или управления действиями человека без использования технических средств. Суть социальной инженерии заключается в применении только психологических методов воздействия на людей, убеждения, внушения доверия и хитрости. В основе методов социальной инженерии всегда лежит манипулирование базовыми эмоциями человека: страхом, жадностью, эмпатией. Основная задача

социального инженера — «подобрать ключ» к каждому конкретному человеку и сыграть на его чувствах и эмоциях так, чтобы он забыл про осторожность и совершил необходимые злоумышленнику действия.

В результате успешных атак с применением методов социальной инженерии жертва добровольно и зачастую без каких-либо подозрений предоставляет злоумышленнику важные данные (логины и пароли от учетных записей, реквизиты банковских карт) или необходимые возможности для получения доступа к целевой системе в обход ограничений безопасности.

Типичным примером атаки социального инженера является звонок или рассылка сообщений клиенту банка от лица сотрудника этого банка. Клиенту сообщают, что его карта заблокирована и под предлогом восстановления карты просят предоставить реквизиты и кодовое слово.

Почему человека считают самым слабым звеном в информационной безопасности? Однозначного ответа нет, но эксперты в этой теме указывают на качества, свойственные большинству из нас, и эмоции, испытываемые многими, – это страх, доверие, алчность, желание помочь ближнему.

Профессор психологии Роберт Чалдини в своем бестселлере «Психология влияния» (1984 г.) описал шесть принципов влияния, которые применяют социальные инженеры:

- Взаимность: предпочитаем платить добром за добро
- Последовательность: придерживаемся убеждений, соответствующих нашим ценностям
- Социальное доказательство: соглашаемся с тем, что делает большинство
- Власть и авторитет: готовы идти за людьми, которым доверяем и которых уважаем
- Симпатия: с удовольствием выполняем просьбы людей, которые нам нравятся
- Дефицит: желаем того, что нам недоступно

Социальные инженеры пользуются тем, что психологические манипуляции не требуют больших затрат и специфических знаний (кроме нескольких психологических приемов), их можно применять в течение длительного времени, а еще их сложно обнаружить. Люди, которые владеют ценной информацией или имеют к ней доступ, сравнимы с доступным плодом: они на виду и до них очень легко дотянуться.

Этим активно пользуются мошенники: согласно отчету Verizon, в 2018 году в 17 % случаев утечка данных произошла именно в результате применения методов социальной инженерии. А Джон Макафи (создатель антивируса McAfee) утверждает, что три четверти инструментов среднего хакера – это методы социальной инженерии и у особо успешных хакеров их доля достигает 90 %.

В арсенале социального инженера много приемов, и очень редко он использует их по одиночке. Скорее, он будет умело их сочетать в зависимости от ситуации, чтобы достичь максимального эффекта.

Фишинг (*fishing*) – техника получения логина и пароля для авторизации в компьютерной системе. С этим видом атаки, вероятно, сталкивался каждый интернет-пользователь. Выглядит это так: вы получаете письмо с просьбой перейти по ссылке или нажать на кнопку. А чтобы вы сделали это наверняка, письмо выглядит как важное сообщение от авторитетного сервиса: платежной системы, банка или любого другого, которому вы доверяете и активно пользуетесь.

Достаточно нажать на ссылку или кнопку, авторизоваться на поддельной странице, и ваши логин с паролем окажутся у мошенников. Самые крупные взломы персональных данных за последнее десятилетие всегда начинались с массовой фишинговой рассылки.

Претекстинг (*pretexting*) – техника атак, где злоумышленник представляется другим человеком и под его видом получает нужные данные. Простейший пример: коллега внезапно звонит с просьбой сообщить информацию, которую знаете только вы. Обычно звонок делают из шумного

помещения, как вариант, ночью, когда жертве трудно определить подлинность голоса. Для этого вида атак важно иметь заготовленный сценарий разговора (обман подразумевает голосовое общение), знать несколько фактов о жертве и действовать максимально быстро, не оставляя времени на размышления.

Поиск информации в открытых источниках – сбор данных в социальных сетях. Там можно узнать Ф. И. О. человека и его родных, телефонные номера, клички питомцев, местонахождение и запланированные поездки.

Плечевой серфинг (*shoulder surfing*) – техника, при которой нужную информацию подсматривают из-за плеча. Проще всего это сделать в местах большого скопления людей: в кафе, общественном транспорте, в зале ожидания аэропорта или вокзала.

Социальная инженерия наоборот (*reverse engineering*) – жертва сама делится конфиденциальной информацией с мошенником. Тому достаточно представиться сотрудником техподдержки банка, сотового оператора или любой другой организации, в которой человек оставил персональные данные. Внутри компании работает другая схема: злоумышленник предлагает услугу, от которой жертва не может или не хочет отказаться, передавая ему свои данные для авторизации или другую ценную информацию.

Троянский конь (или *«дорожное яблоко»*) – использование физических носителей информации, которые подбрасывают потенциальной жертве (ею может стать любой человек). Флешка или диск «случайно» появляются там, где их легко найти, а чтобы повысить их шансы быть найденными, мошенники наносят на них логотип компании или делают интригующую надпись. Жертве очень хочется узнать, что же находится на носителе, она вставляет его в компьютер и дальше можно не объяснять, что происходит.

Что будет делать среднестатистический мошенник, чтобы получить информацию о компании с помощью социальной инженерии? Он точно изучит активность ее сотрудников в социальных сетях, просмотрит общедоступные видеоролики и текстовые упоминания об организации. Вероятно, обратится к фишингу, а если позволят обстоятельства. просто подсмотрит данные для авторизации. Люди до сих пор записывают пароли на стикерах и приклеивают их монитор, пользуются корпоративными сервисами в открытых Wi-Fi-сетях. Заметьте, чтобы получить информацию этими способами, мошеннику даже не придется применять сложные психологические приемы или втираться в доверие к потенциальной жертве!

Представьте себя в роли социального инженера, которому нужно получить ценную информацию. Тогда дорожная карта будет выглядеть следующим образом:

1. Сбор информации. Начальные сведения помогут ближе изучить цель и понять, с чем вы имеете дело. Подойдут активные и пассивные методы по методологии OSINT (Open source intelligence) – разведки на основе открытых источников. К открытым источникам относятся СМИ, публикации в интернете, общедоступные данные аэросъемок и радиомониторинга, публичные отчеты государственных и коммерческих организаций, профессиональные отчеты, конференции, доклады
2. Выбор жертвы – человека, слабости которого будут вам полезны. Лучшими претендентами на эту роль станут те, кого легко обмануть, ввести в заблуждение, люди с чувством обиды или выраженной эмпатией
3. Подготовка технического решения для фишинга. Самая трудоемкая и затратная часть в социальной инженерии, которая включает регистрацию домена, хостинга, их настройку и обкатку
4. Контакт. Войти в круг доверия жертвы

На финальном этапе вы используете полученную информацию для достижения заветной цели: например, узнать пароль к системе или схему расположения камер видеонаблюдения. В отличие от других мошенников вам, вероятно, не придется заметать следы. Даже если жертва осознает собственный промах, она вряд ли поделится этой информацией с руководством, ведь признаваться в собственной глупости – занятие не самое приятное.

Методы защиты от социальной инженерии. Защищаться от техник социальной инженерии сложно, так как жертвы часто не догадываются о том, что их обманули и использовали их слабости, чтобы заполучить конфиденциальную информацию. Решить проблему можно одним способом: повысить осознанность сотрудников. А для этого их придется обучить правилам работы с информацией и донести опасность ее раскрытия. Вот что для этого можно сделать.

Определить информацию, уязвимую к атаке. Сотрудники должны уметь классифицировать информацию по степени защищенности и понимать, раскрытие каких данных может причинить вред компании. Например, пользовательские учетные данные всегда принадлежат организации, их нельзя передавать третьим лицам или оставлять в открытом доступе. Значит, придется распрощаться со стикерами, где написаны логины/пароли, не авторизовываться на корпоративных ресурсах через открытые Wi-Fi-сети. Также помогает привычка блокировать ПК или ноутбук в свое отсутствие.

Повысить компетентность в вопросах информационной безопасности. Техники социальной инженерии постоянно совершенствуются, а кибермошенники находят новые способы сыграть на человеческих эмоциях. Потому сотрудникам компании необходимо знать, жертвами каких потенциальных атак они могут стать и как вести себя в подобных ситуациях. Например, куда следует написать/позвонить, если

третьи лица запросили у них конфиденциальную информацию или данные для авторизации.

Ограничить права доступа к информационным системам. Доступ на копирование, скачивание, изменение информации должны иметь только те сотрудники, которым это необходимо для выполнения должностных обязанностей. В некоторых компаниях целесообразно запретить использование съемных носителей.

Подготовить инструкции по обмену информацией. В любом отделе и подразделении все – от рядового офисного сотрудника до руководителя – должны иметь четкие инструкции о том, в каких условиях они могут раскрыть важную для компании информацию. В инструкции можно указать, какие сведения можно передавать службам техподдержки, представителям контролирующих органов и т. п.

Обновить антивирусное ПО до актуальной версии. Это поможет сделать компьютеры сотрудников менее уязвимыми к массовым фишинговым атакам. Современное антивирусное ПО включает инструменты для защиты от шпионских и вредоносных программ, и предупреждает при переходе по подозрительным ссылкам. Впрочем, доступа к социальным сетям на рабочем месте лучше не давать – это первое, чем обязательно воспользуются социальные инженеры.

Если речь идет о компании, то все сотрудники должны быть предупреждены об опасности раскрытия персональной информации и конфиденциальной информации компании, а также о способах предотвращения утечки данных. Лучше всего это реализовать с помощью разработки четких и ясных инструкций, в которых будет прописано, какую информацию можно предоставлять другим лицам (посетителям, коллегам, в службу технической поддержки).

Существует несколько дополнительных правил вышеперечисленным методом защиты от атак социальной инженерии, которые следует неукоснительно соблюдать всем пользователям.

1. Никому и никогда не сообщать логины и пароли от своих учетных записей. Даже если пытаются убедить, что от этого зависит выполнение срочной и важной задачи. Помнить, что сотрудники банка не имеют права запрашивать номер банковской карты, CVV/CVC-код и иную информацию, позволяющую произвести списание денежных средств.
2. Не скачивать вложения и не переходить по подозрительным ссылкам в письмах, полученных даже от известных лиц. Всегда проверять с помощью других доступных каналов связи (телефонного звонка, сообщения в мессенджере), что отправитель письма — именно тот, за кого себя выдает.
3. Перед переходом по ссылке из письма или сообщения навести на неё курсором мыши, чтобы увидеть реальный URL-адрес страницы.
4. Блокировать компьютер, перед выходом от своего рабочего места.
5. Использовать надежные и уникальные пароли для различных сервисов. Использовать менеджеры паролей.

Нужно помнить от атак социальных инженеров позволит защититься только личная бдительность и критический подход, а также правильно настроенная политика кибербезопасности. Это может включать в себя политику обнаружения атак, политика использования электронной почты.

Политика использования электронной почты

Электронная почта одно из самых важных средств коммуникации в деловом мире. Сообщения быстро и удобно передаются по внутренним сетям и всему миру через интернет. Тем не менее, существуют риски при ведении бизнеса с помощью электронной почты, так как по сути электронная почта небезопасна, особенно за пределами корпоративной сети. Сообщения могут быть перехвачены, записаны, прочитаны, изменены и перенаправлены кому угодно, а иногда просто пропасть. Случайные комментарии могут быть поняты неправильно и привести к нарушению контрактов или судебным разбирательствам.

Основные принципы

А. Пользователи электронной почты должны избегать деятельность, нарушающую информационную безопасность.

Б. Корпоративная электронная почта должна использоваться в рамках должностных обязанностей. Все сообщения электронной почты в информационных системах и сетях считаются собственностью компании.

Требования политики

1. Не используйте электронную почту:

- Для отправки конфиденциальной/секретной информации если она не зашифрована криптографическим ПО, разрешенным к использованию в компании;
- Для создания, отправки, пересылки или хранения сообщений или вложений, которые могут считаться незаконными или оскорбительными простыми людьми, например, материалы сексуального характера, расистские, дискредитирующие, оскорбительные, непристойные, уничижительные, дискриминационные, угрожающие, беспокоящие или иные подобные сообщения;
- Для установления отношений с третьими сторонами, например, для заключения контрактов на покупку или продажу, отправки предложений о работе или прайс-листов, если это не входит в ваши служебные обязанности. Не изменяйте и не удаляйте уведомления, автоматически вставляемые в конце писем;
- В личных и благотворительных целях, не связанных с бизнесом организации;
- Образом, который может быть интерпретирован как официальная позиция или высказывание организации;
- Для отправки сообщения с чужого почтового ящика или от чужого имени (включая использование поддельного поля «ОТ»). Если это позволено руководством, секретарь может отослать письмо от имени

сотрудника, подписав письмо собственным именем, указав по чьему поручению оно было отправлено.

- Для рассылки любых подрывных, оскорбительных, неэтичных, незаконных или иначе недопустимых материалов, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возрасте, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений или о национальном происхождении, гиперссылок или других ссылок на неприличные или очевидно оскорбительные веб-сайты и подобные материалы, шутки, массовые рассылки, предупреждений о вирусах и розыгрышей, обращений о помощи, вирусов или другого злонамеренного программного обеспечения;
- В любых других незаконных, неэтичных и неразрешенных целях.

2. Проявляйте профессиональное благоразумие при использовании электронной почты. Придерживайтесь общепринятых правил этикета при работе с электронной почтой (см. Правила безопасности электронной почты). Тщательно проверяйте сообщения перед отправкой, особенно при общении с внешними контрагентами.

3. Не раскрывайте без необходимости возможно непубличную информацию в сообщениях, уходящих за пределы компании.

4. Сообщения электронной почты автоматически сканируются в информационных системах на наличие вредоносных программ, спама и нешифрованной служебной или личной информации. К сожалению, процесс сканирования недостаточно эффективен (например, сжатые и шифрованые сообщения не могут быть полностью просканированы), поэтому нежелательная/сомнительная почта иногда попадает к пользователям. Удаляйте такие сообщения или сообщайте о них в службу поддержки.

5. Сотрудники не должны перехватывать, игнорировать, изменять, удалять, сохранять или публиковать сообщения кроме случаев,

санкционированных руководством или в целях администрирования ИТ систем.

6. Ограниченное использование корпоративной электронной почты разрешается под ответственность руководства, учитывая, что это носит случайный и непостоянный характер и не мешает выполнению должностных обязанностей. Все сообщения, отправляемые в корпоративных системах и сетях подвергаются автоматическому сканированию и могут быть помещены в карантин и/или просмотрены уполномоченными сотрудниками.

7. Не используйте веб-сервисы Gmail, Hotmail, Yahoo или похожие почтовые системы третьих сторон (обычно называемые «вебмайл») в служебных целях. Не пересылайте и не перенаправляйте корпоративную электронную почту на внешние почтовые системы/системы третьих сторон. Вы можете пользоваться вашим личным почтовым ящиком с использованием корпоративных систем под ответственность руководства с учетом, что этот вид использования почты крайне ограничен и не считается личным использованием (см. выше).

8. Рационально подходите к числу и размеру сообщений которые вы отправляете и храните. Периодически очищайте ваш почтовый ящик, удаляя старые сообщения, которые больше не нужны и перемещая необходимые сообщения в соответствующие почтовые папки. Отправляйте важные письма в архив в соответствие с политикой архивирования почты.

Ответственность

Управление информационной безопасности отвечает за соблюдение требований настоящей политики. Будучи в тесной связи с другими бизнес-функциями управление ответственно за образовательную деятельность, имеющую целью повысить уровень осведомленности и понимания ответственности, обозначенной в данной политике.

Департамент ИТ отвечает за организацию, конфигурирование, использование и обслуживание оборудования для работы с электронной

почтой (включая антиспам, антивирус и другие фильтры) в соответствие с данной политикой.

Служба ИТ поддержки отвечает за помощь сотрудникам в использовании электронной почты и служит центральным пунктом сбора сообщений об инцидентах с использованием электронной почты.

Все сотрудники, имеющие отношение к настоящей политике, несут ответственность за соблюдение данной и остальных корпоративных политик. Настоящая политика также относится к сотрудникам третьих организаций, работающих в тех же условиях независимо от того связаны ли они с политикой информационной безопасности компании явно (например, особыми пунктами контрактов) или не явно (например, общепринятыми нормами поведения).

Компания имеет право оценки выполнения требований настоящей политики в любое время.

Таблица № 1. Соответствие политик, стандартов и правил

Соответствие	
Описание политик информационной безопасности	Описывает набор правил безопасности в соответствие с ISO/IEC 27002, международным стандартным документом по практике управления информационной безопасностью
Политика архивирования электронной почты	Разъясняет правила создания резервных копий, архивов и восстановления важных сообщений
Правила безопасного использования электронной почты, лучшие решения и т. д.	Основные советы пользователям электронной почты, впервые выпедшие в сентябре 2007 года в рамках программы ознакомления с правилами информационной безопасности. Включает в себя правила почтового этикета, обращение с мошенническими и содержащими вирусы письмами и т. д.

Контакты

За дальнейшей информацией по настоящей политике и соблюдению требований информационной безопасности в целом, обращайтесь к менеджеру по информационной безопасности. Различные стандарты,

процедуры, правила и другие материалы в отношение настоящей и других политик информационной безопасности находятся в справочнике по информационной безопасности организации, на корпоративном интранет-сайте и у менеджера по информационной безопасности. Сотрудники департамента ИТ и информационной безопасности также могут оказать поддержку при применении этой политики, обращайтесь к своему начальнику или в службу техподдержки.

Практическая часть

В данной практической работе мы разберем принцип работы средств защиты от социальной инженерии на примере программного средства SET. Основой информационной безопасности является системное мышление, в основе которого лежит мышление как злоумышленник. Исходя из этого, сегодня мы рассмотрим создание фишингового сайта с помощью программного обеспечения SET, доступного в инструментарии операционной системы Linux.

Social Engineering Toolkit (SET) — это бесплатный инструмент с открытым исходным кодом, который используется для атак социальной инженерии, таких как фишинг, подделка телефонных номеров, отправка SMS и т. д. Этот бесплатный инструмент, доступен в Kali Linux, или вы можете напрямую загрузить и установить его с Github.

Social Engineering Toolkit (SET) разработан и разработан программистом по имени Дэйв Кеннеди. Этот инструмент используется исследователями безопасности и тестировщиками на проникновение по всему миру для проверки недостатков кибербезопасности в системах. Набор инструментов социальной инженерии предназначен для выполнения атакующих методов на их машинах. Этот набор инструментов также предлагает векторные атаки на веб-сайты или пользовательские векторные атаки, с помощью которых вы можете клонировать любой веб-сайт и выполнять фишинговые атаки.

Особенности инструментария социальной инженерии:

- SET является бесплатным и открытым исходным кодом
- SET является переносимым, что означает, что вы можете легко изменить вектор атаки.
- SET — это многоплатформенный инструмент: он может работать в Linux, Unix и Windows.
- SET поддерживает интеграцию со сторонними модулями.
- SET включает доступ к платформе Fast-Track для тестирования на проникновение.
- SET предоставляет множество векторов атак, таких как целевые фишинговые атаки, атаки на веб-сайты, генератор инфекционных носителей и т. д.

Использование инструментария социальной инженерии:

- **Фишинговые атаки:** Social Engineering Toolkit позволяет проводить фишинговые атаки на вашу жертву. Используя SET, вы можете создавать фишинговые страницы многих веб-сайтов, таких как Instagram, Facebook, Google и т. д. SET сгенерирует ссылку на выбранный вами вариант, а затем вы сможете отправить этот URL-адрес жертве, как только жертва откроет этот URL-адрес. и он / она увидит законную веб-страницу реального веб-сайта, которая на самом деле является фишинговой страницей. Как только он / она введет свой идентификационный пароль, вы получите этот идентификационный пароль на экране своего терминала. Вот как работает фишинговая атака с использованием SET.
- **Веб-атака:** Веб-атака — это модуль в SET. Этот модуль сочетает в себе различные варианты удаленной атаки на жертву. С помощью этого модуля вы можете создать полезную нагрузку и доставить полезную нагрузку в браузер жертвы с помощью эксплойта браузера Metasploit. веб-атака имеет метод Credential Harvester, с помощью которого вы можете клонировать любой веб-сайт для фишинговой

атаки и можете отправить ссылку на эту веб-страницу жертве для сбора информации из полей пользователя и пароля.

- **Создайте полезную нагрузку и прослушиватель:** когда вы впервые запустите инструментарий социальной инженерии. Вы увидите 4-й вариант, который заключается в создании полезной нагрузки и прослушивателя с помощью этого модуля SET, вы сможете создавать вредоносные полезные нагрузки для Windows, включая Shell Reverse_TCP, Reverse_TCP Meterpreter, Shell Reverse_TCP X64 и Meterpreter Reverse HTTPS. Вы можете использовать эти полезные нагрузки так же, как вы используете полезные нагрузки из metasploitable.
- **Mass Mailer Attack** : массовая почтовая атака — это модуль в наборе инструментов социальной инженерии, который используется для бомбардировки электронных писем на целевой почтовой учетной записи, для чего вы также можете использовать свою собственную учетную запись Gmail или иметь для этого сервер.

Это были некоторые векторы атак, которые вы можете выполнить с помощью Social Engineering Toolkit. Когда вы запустите SET, вам будет весело, потому что использовать SET очень просто, теперь мы увидим, как вы можете установить Social Engineering Toolkit и как вы можете использовать его для фишинговой атаки.

Атака с использованием социальной инженерии для получения доступа к электронной почте

Цель атаки получение информации об учетных записях электронной почты. Для этого нужно иметь компьютер или ноутбук с Kali Linux, и мобильный телефон в качестве устройства предоставляющую доступ к интернету.

Итак, исходя из сценария выше, вы можете себе представить, что нам даже не нужно устройство жертвы. Нужна только его доверие, и глупость.

В этом случае сначала нужно настроить фишинговую страницу входа в учетную запись Gmail в Kali Linux и использовать телефон в качестве триггерного устройства.

Шаг 1. Настройка фишинг-страницы

Setoolkit использует интерфейс командной строки. Откройте терминал и введите:

```
~# setoolkit
```

Вы увидите страницу приветствия вверху и параметры атаки внизу (Рис.№7.1).

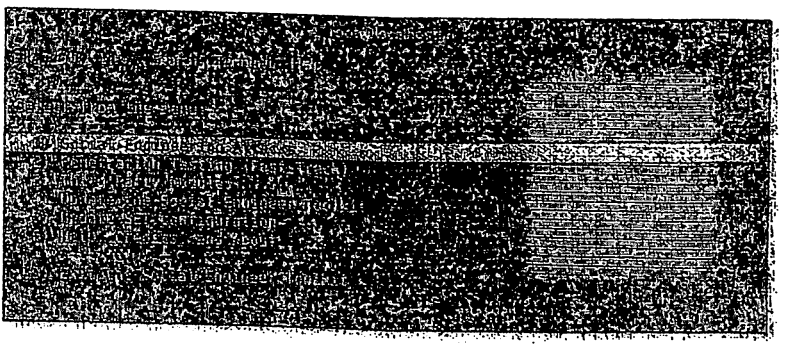


Рис.7.1. Параметры атаки Social Engineering Toolkit.

Будем проводить атаки социальной инженерии, поэтому выберите номер 1 и нажмите Enter.

Затем вам будут показаны следующие варианты, и выберите номер 2 векторы атак на веб-сайты (Рис.№7.2). Нажмите Enter.

Далее выбираем номер 3-Метод атаки Credential Harvester (Рис.№7.3). Нажмите Enter.

Дополнительные параметры более узкие, SET имеет предварительно отформатированные фишинговые страницы популярных веб-сайтов, таких как Google, Yahoo, Twitter и Facebook. Теперь выберите номер 1 Веб-шаблоны (Рис №7.4.).

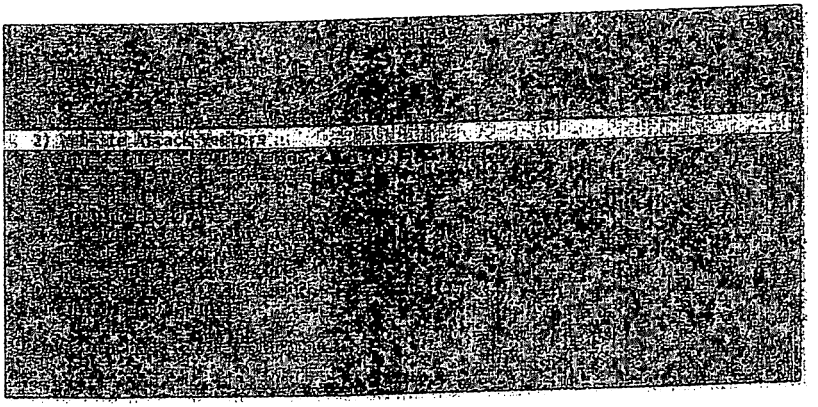


Рис.7.2. Векторы атак на веб-сайты

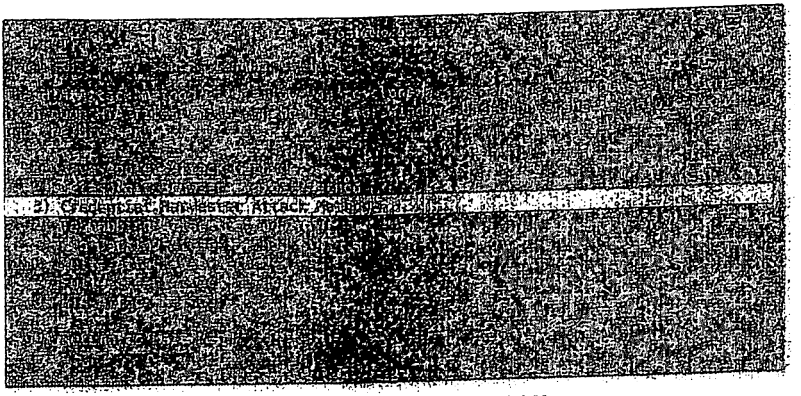


Рис.7.3. Выбор метода атаки Credential Harvester

Поскольку ПК с Kali Linux и мобильный телефон находились в одной сети Wi-Fi, нужно просто ввести локальный IP-адрес злоумышленника (Рис №7.5). И нажмите Enter.

Итак, мы установили наш метод и IP-адрес слушателя. В этих опциях перечислены предопределенные шаблоны веб-фишинга, как было упомянуто выше. Поскольку мы нацелились на страницу аккаунта Google, поэтому нужно выбрать номер 2. Google и нажать Enter (Рис.№7.6). После этого будет происходит клонирование сайта Google (Рис.№7.7).

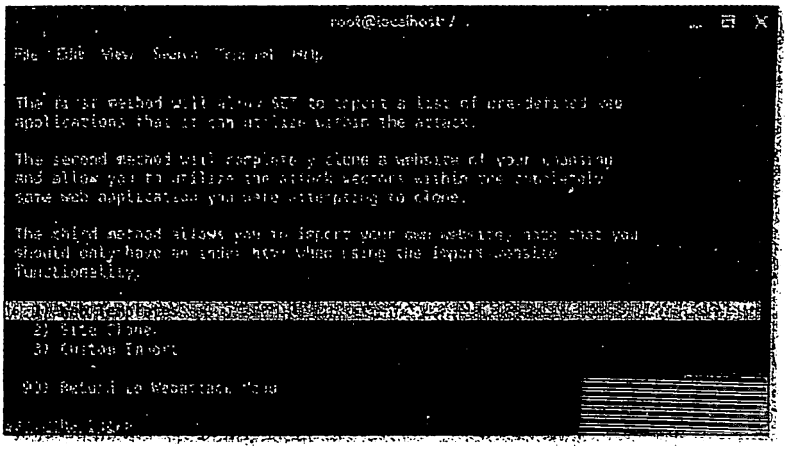


Рис.7.4. Выбор веб шаблонов.

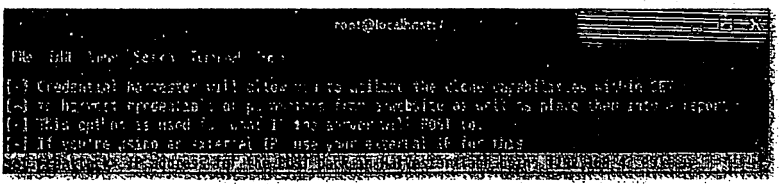


Рис.7.5. Ввод адреса злоумышленника.

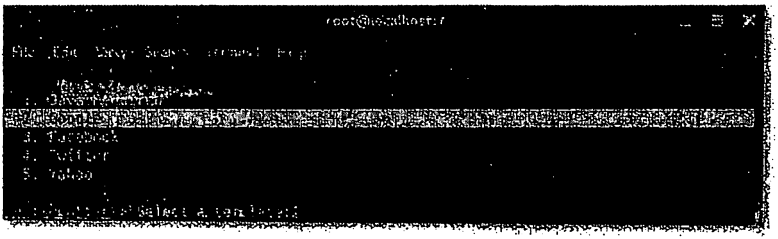


Рис.7.6. Выбор страницы.

Рис.7.7. Процесс клонирования.

Теперь SET запускает веб-сервер Kali Linux на порту 80 с поддельной страницей входа в учетную запись Google. На этом установка завершена.

Шаг 2. Охота на жертв

Давайте посмотрим, как страница отображается в встроенном браузере Android. Итак, заходим на веб-сервер Kali Linux по адресу **192.168.43.99** в браузере. А вот и страница (Рис №7.8):

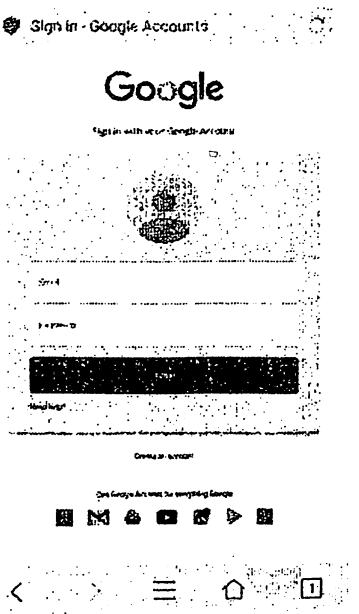


Рис.7.8. Поддельная страница.

Он выглядит настолько реальным, что на нем нет никаких проблем с безопасностью. Строка URL-адреса, показывающая заголовок вместо самого URL-адреса. Мы знаем, что простые пользователи узнают это как оригинальную страницу Google.

Итак, взяв мобильный телефон, можете подойти к своему другу и сказать как будто Вам не удалось войти в Google, и действуете, так что Вам интересно, не произошел ли сбой или ошибка Google. Дайте телефон и просите его попробовать войти, используя его учетную запись. Он, поверив словам сразу начинает вводить данные своего аккаунта, как будто ничего страшного здесь не произойдет. Как только жертва нажмет кнопку «Войти», идёт загрузка и страница отправит информацию для аутентификации на компьютер-слушатель и войдет в систему. Далее появляется главная страница поисковой системы Google (Рис.№7.9.)

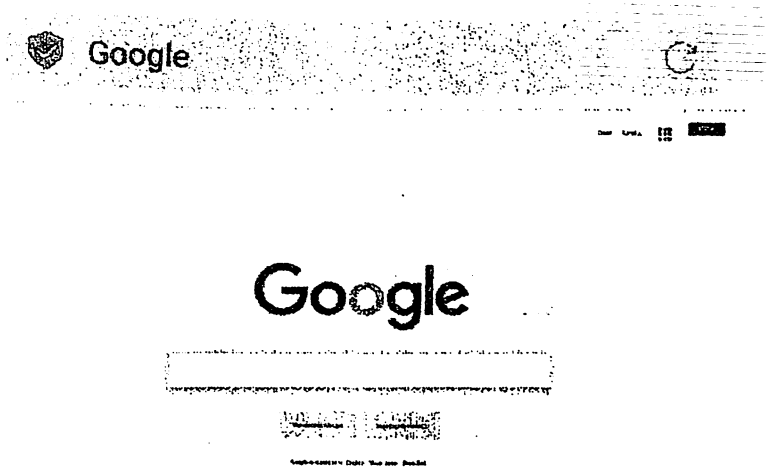


Рис.7.9. Переход в страницу поисковой службы.

После этого вы можете проверить журнал SET. И вот что было получено (Рис№7.10):

Рис.7.10. База аккаунтов и паролей которая была получена с помощью SET.

Атака, проведенная нами, показывает, что интернет-пользователи действительно доверчивы и уязвимы для фишинговых атак. Из этого следует, что мы можем получить некоторый результат от атак социальной инженерии, только если мы будем проводить постоянные разъяснительные работы и семинары касаемые работе в Интернете. Никакие технические средства защиты данных не помогут если пользователи не проинформированы правилами работы в Интернете.

Задание:

1. Провести фишинговую атаку с помощью набора инструментов.
2. Проанализировать как можно защититься такого рода атак.

Контрольные вопросы:

1. Что представляет собой описание политик информационной безопасности использования электронной почты?
2. Какими уязвимостями пользователей пользуются злоумышленники? Чем опасны атаки социальной инженерии?
3. Как работает набор инструментов Social Engineering Toolkit?
4. Что должен быть включен в программно-аппаратных средствах во всех хостах и серверах?

Содержание

Составители:

Зокиров О.Ё	и.о. доцент кафедры «Кибербезопасность и криминалистика», ТУИТ
Муминова С.Ш.	старший преподаватель кафедры «Кибербезопасность и криминалистика», ТУИТ
Юлдашева Н.С	ассистент кафедры «Кибербезопасность и криминалистика», ТУИТ

Методические указания рассмотрены и одобрены на заседании кафедры "Обеспечение информационной безопасности"
(__ _____ 2022 г. Протокол № _____)

Методические указания рекомендованы к печати на заседании научно-методического совета факультета "Информационная безопасность"
(__ _____ 2022 г. Протокол № _____)

Методические указания утверждены на Научно-методическом совете Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий
(__ _____ 2022 г. Протокол № _____)

Формат 60x84 1/16. Печ.лист 8.
Заказ № 70. Тираж 15.
Отпечатано в «Редакционном издательском»
Отеле при ТУИТ
Ташкент ул.Амир Темур, 108