Введение

Современный мир невозможно представить без средств коммуникаций и вычислительной техники, где главенствующую роль играет программное обеспечение. Информационные технологии прогрессируют очень быстро, охватывая все более широкие области человеческой деятельности. Поэтому безопасность информационных технологий является одним из важнейших аспектов обеспечения их функционирования.

Рост числа компьютеров и компьютерных сетей, все более широкое использование сетевых технологий и технологии Интернета не только значительно расширили географию пользователей, их возможности по общению друг с другом, но и увеличили возможность реализации сетевых бизнес-процессов. Организации, компании и рядовые пользователи получили возможность использовать технологии Интернета в повседневной деятельности. Этому способствует развитие существующих служб и появление новых, востребованных мировым сообществом. Кроме возрастающих возможностей использование интернет-технологий значительно увеличивает и риск потери данных, потери репутации и просто финансовые потери. Целью настоящего практикума является рассмотрение ряда основных практических задач обеспечения информационной безопасности в организации.

Рассматриваемые в лабораторных работах задания, позволяют ознакомиться с методами и технологиями проектирования, моделирования, исследования автоматизированных систем и их подсистем безопасности, получить навыки использования программно-аппаратных средств обеспечения информационной безопасности. Этому посвящены практические занятия в практикуме. В современных условиях аудит информационной безопасности представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента (управления) в области безопасности информационных систем. Основная задача аудита — объективно оценить текущее состояние информационной безопасности (ИБ) компании, а также ее адекватность поставленным целям и задачам для увеличения эффективности деятельности организации.

Практическое занятие № 1

Исследование корректности систем защиты

Цель работы: приобрести начальные практические навыки исследования систем защиты.

Задание: провести исследование стойкости парольных систем защиты: системы идентификации и аутентификации ОС Windows XP; архивов; документов MS office. Провести исследование систем стенографической защиты и специальных систем поиска, восстановления и безвозвратного уничтожения конфиденциальных файлов.

Исследование стойкости системы идентификации ОС Windows XP

1. Установить пароли на ОС Windows XP.
2. С помощью специализированной программы из предоставленных CD-диска взломать пароли ОС Windows XP и получить доступ в систему от имени администратора. В отчете записать примерное время взлома.

Исследование стойкости запароленных архивов

1. Исследование стойкости запароленных архивов *.RAR:
   а) с помощью программы WINRAR создать запароленный на 3, 4, 5, 6 символов с английскими и (или) русскими символами архив любого текстового файла и сохранить его на Рабочем столе;
   б) провести инсталляцию программы ARCHPR 2.0;
   в) после этого, попытаться разархивировать запароленный архив, воспользовавшись установленной программой;
   г) в отчете записать успешные и безуспешные попытки, указав примерное время взлома.

2. Исследование стойкости запароленных архивов *.ZIP:
   а) с помощью программы WINZIP создать запароленный на 3, 4, 5, 6 символов с английскими и (или) русскими символами архив любого текстового файла и сохранить его на Рабочем столе;
   б) провести инсталляцию программы ARCHPR 2.0;
   в) после этого попытаться разархивировать запароленный архив, воспользовавшись установленной программой;
   г) в отчете записать успешные и безуспешные попытки, указав примерное время взлома.

Исследование стойкости паролей MS Office

1. С помощью штатных средств Microsoft Word запаролить текстовый файл на открытие тремя методами с длиной пароля 2–6 символов.
2. С помощью специальной программы попытаться взломать пароль. В отчете записать успешные и безуспешные попытки, указав примерное время взлома.

Методика практической реализации поиска, восстановления и безвозвратного уничтожения конфиденциальных файлов

1. Создать на *Рабочем столе* текстовый файл.
2. Уничтожить файл с помощью средств ОС.
3. С помощью специальных программ попытаться восстановить файл, открыть восстановленный файл, проверить корректность восстановления файла, подобрать программу, которая правильно восстановит файл, записать результаты со временем восстановления.
4. Уничтожить файл с помощью специальной программы.
5. С помощью специальных программ попытаться восстановить файл, записать результат.

Методика практической реализации стенографической защиты

1. Создать на *Рабочем столе* текстовый файл.
2. С помощью папки *Стеганография* зашифровать его в графический файл из системной папки Windows с использованием различных программ.
3. Расшифровать файл.

Описание программно-аппаратной среды

1. Операционная система Windows XP (7).
2. Виртуальная машина VMware.
3. СПО ARCHPR 2.0, Advanced Office 2000 Password Recovery, Stegosaurus, EasyRecovery Professional.
4. ПО MS Office.

Указания по выполнению работы

В настоящее время для защиты информации от несанкционированного доступа часто применяются такие методы, как идентификация, аутентификация и используемое при их реализации криптографическое преобразование информации.

Идентификация — это присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных.

Аутентификация — это проверка принадлежности пользователю предъявленного им идентификатора. Часто аутентификацию также называют подтверждением или проверкой подлинности.

Наиболее распространенные методы аутентификации основаны на применении многоразовых или одноразовых паролей. Эти методы включают следующие разновидности способов аутентификации:

- по хранимой копии пароля или его свертке (*plaintext-equivalent*);
- по некоторому проверочному значению (*verifier-based*);
- без непосредственной передачи информации о пароле проверяющей стороне (*zero-knowledge*);
- с использованием пароля для получения криптографического ключа (*cryptographic*).

В первую разновидность способов входят системы аутентификации, предполагающие наличие у обеих сторон копии пароля или его свертки. Для организации таких систем требуется создать и поддерживать базу данных, содержащую пароли или сверки паролей всех пользователей. Слабой стороной этого способа является то, что злоумышленник, получив доступ к базе данных, сможет проходить аутентификацию от имени любого пользователя [1].

Способы, составляющие вторую разновидность, обеспечивают более высокую степень безопасности парольной системы, так как проверочные значения, хотя они и зависят от паролей,

не могут быть непосредственно использованы злоумышленником для аутентификации.

Наконец, аутентификация без предоставления проверяющей стороне какой бы то ни было информации о пароле обеспечивает наибольшую степень защиты. Этот способ гарантирует безопасность даже в том случае, если нарушена работа проверяющей стороны (например, в программу регистрации в системе внедрен «троянский конь»).

Особым подходом в технологии проверки подлинности являются криптографические протоколы аутентификации, описывающие последовательность действий, которую должны совершить стороны для взаимной аутентификации. Кроме того, эти действия, как правило, сочетаются с генерацией и распределением криптографических ключей для шифрования последующего информационного обмена. Корректность протоколов аутентификации вытекает из свойств задействованных в них математических и криптографических преобразований и может быть строго доказана.

В руководящих документах рекомендуется в АС, обрабатывающих конфиденциальную информацию и информацию, содержащую сведения, составляющие государственную тайну, устанавливать длину пароля не менее 6–8 сложных цифрознаков.

База данных об учетных записях пользователей и их паролях в ОС Windows, начиная с версии NT 4.0 и выше, включая Windows 7, хранится в SAM-файле из директории C:\Windows\system32\config.

При работающей ОС Windows этот файл недоступен для изменения и доступа. Но в DOS-режиме он вполне доступен для изучения и изменения. Как следствие, существуют специальные программы, позволяющие взламывать или стирать пароли пользователей. Одной из них является Active Password Changer из состава Hiren's BootCD, бесплатно распространяемого через Интернет.

Итак, вставляем диск Hiren's BootCD в CD-дисковод и загружаемся с него. Этот диск содержит огромный спектр программ и утилит. Мы воспользуемся программой Active Password Changer (рис. 1).

Поскольку на компьютере может быть установлено несколько ОС на разных логических дисках, следует определиться, в какой ОС следует уничтожать пароли. Для поиска всех имеющихся SAM-файлов (содержащих пароли пользователей в зашифрованном виде) во всех установленных ОС следует выбрать опцию

Search for MS SAM Dadtbase on all hards disks and logical drives. Далее программа показывает результаты поиска, после чего следует нажать клавишу ВВОД.

Рис. 1. Окно программы *Hirens BootCD*

На рис. 2 видно, что данный SAM-файл содержит три записи пользователей. Для изменения атрибутов, например регистрационной записи под номером 0, следует нажать клавишу 0, затем ВВОД.

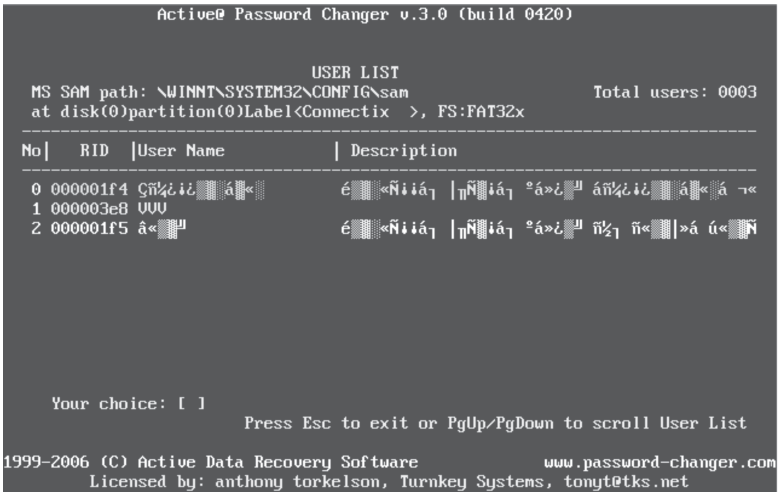

Рис. 2. Окно программы *Active Password Changer* с найденными записями паролей пользователей

В следующем меню программы уже непосредственно меняем атрибуты учетной записи, для этого ставим знак X в нужном

разделе. Программа позволяет уничтожить существующий пароль к учетной записи, а также изменить пароль на свой, заблокировать или совсем отключить учетную запись. Для сохранения настроек следует нажать клавишу *Y* (*Yes*) и перезагрузить компьютер (рис. 3). Таким образом, барьер в виде защиты ОС паролем стандартными средствами был преодолен с помощью специального программного обеспечения.

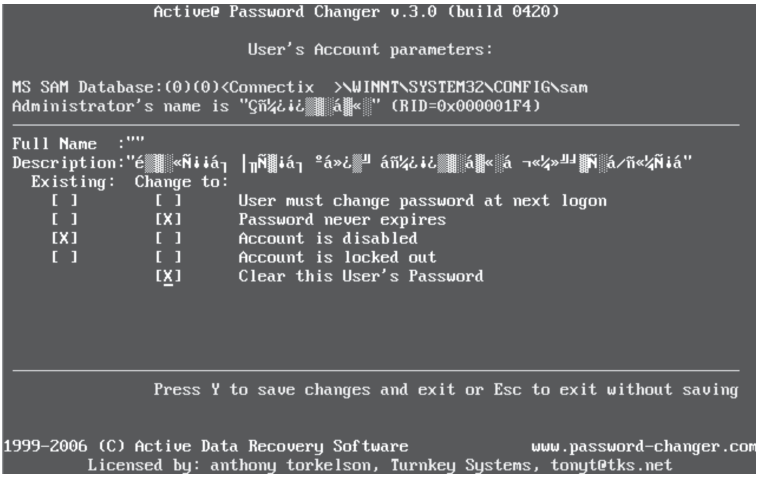

Рис. 3. Окно программы *Active Password Changer* с изменяемыми атрибутами свойств парольных записей

Естественной и, пожалуй, единственной защитой от подобных программ является установка пароля на BIOS и запрет загрузки с внешних носителей.

Исследование стойкости парольных систем защиты архивов

Изначально потребность в архивировании информации возникла в результате необходимости экономии дискового пространства машинных носителей.

В процессе развития и совершенствования программ для архивирования как отдельная сервисная функция возникла возможность установки пароля на архивный файл. Это оказалось очень удобным, ведь появилась дополнительная функция защиты. Однако пароли достаточно часто забываются и утрачиваются. В связи с этим появились программы восстановления паролей