Некоммерческое акционерное общество

АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ

Кафедра инженерной кибернетики

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ УПРАВЛЕНИЯ

Методические указания по выполнению лабораторных работ
для студентов специальности 5В070200 – Автоматизация и управление

Алматы 2017

СОСТАВИТЕЛИ: К.Т.Сауанова. Методы защиты информации в системах управления. Методические указания по выполнению лабораторных работ для студентов специальности 5В070200 – Автоматизация и управление. – Алматы: АУЭС, 2017. – 38 с.

Методические указания содержат указания по выполнению лабораторных работ, в них приведены краткие теоретические сведения, задания и контрольные вопросы по каждой лабораторной работе, дана методика выполнения, приведен перечень рекомендуемой.

Методические указания предназначены для студентов всех форм обучения специальности 5В070200 –Автоматизация и управление.

Ил.__, табл. 2 , библиогр. – 7 назв.

Рецензент: доц.А.А.Аманбаев.

Печатается по плану издания некоммерческого акционерного общества «Алматинский университет энергетики и связи» на 2017 г.

©НАО «Алматинский университет энергетики и связи», 2017 г.

Введение

Проведение лабораторных работ предусмотрено учебной программой подготовки специалистов направления 5В070200.

Основными задачами лабораторных работ по дисциплине «Методы защиты информации в системах управления» являются:

- закрепление теоретических знаний, полученных на лекционных занятиях по изучаемой дисциплине;
- изучение основных понятий и определений защиты компьютерной информации. Законодательно – правовые и организационные методы защиты компьютерной информации;
- изучение современных методов и средств защиты компьютерной информации, их использование в практической деятельности;
- обучение самостоятельной работе с нормативно-справочной литературой, проявляя при этом инициативу и стремление к получению новых знаний и навыков в области защиты компьютерной информации.

1 Лабораторная работа №1. Количественная оценка стойкости парольной защиты

Цель: реализация простейшего генератора паролей, обладающего требуемой стойкостью к взлому.

Теоретические сведения.

Подсистемы идентификации и аутентификации пользователя играют важную роль в системах защиты информации.

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

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

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

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

Типы угроз безопасности парольных систем:

1) Разглашение параметров учетной записи через:

- подбор в интерактивном режиме;
- подсматривание;
- преднамеренную передачу пароля его владельцем другому лицу;
- захват базы данных парольной системы (если пароли не хранятся в базе в открытом виде, для их восстановления может потребоваться подбор или дешифрование);
- перехват переданной по сети информации о пароле;
- хранение пароля в доступном месте.

2) Вмешательство в функционирование компонентов парольной системы:

- внедрение программных закладок;
- обнаружение и использование ошибок, допущенных на стадии разработки;
- выведение из строя парольной системы.

Некоторые из перечисленных типов угроз связаны с наличием так называемого человеческого фактора.

Минимальные требования к подсистемам парольной аутентификации пользователя следующие:

К паролю:

1) Длина пароля не менее 6 символов.

2) Пароль содержит символы из различных групп символов (большие и маленькие латинские буквы, цифры, специальные символы и т.д).

3) В качестве пароля не должны использоваться осмысленные слова, имена родственников, фамилия и другая личная информация.

К подсистеме аутентификации:

1) Ограничение срока действия пароля.

2) Ограничение на количество попыток ввода пароля.

3) Временная задержка при вводе неправильного пароля.

4) Отправка сообщения на личный телефон при вводе неправильного пароля.

При выдержке перечисленных выше требовании возможными способами несанкционированного доступа является подбор пароля методом перебора (brute forcing) и атака по словарю.

Защищенность пароля при его подборе зависит, в общем случае, от скорости проверки паролей и от размера полного множества возможных паролей, которое, с свою очередь, зависит от длины пароля и мощности алфавита символов. Количественная оценка стойкости парольной защиты.

Пусть A – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля: если пароль состоит только из малых английских букв, то $A = 26$); L – длина пароля; $S = A^L$ – число всевозможных паролей длины L, которые можно составить из символов алфавита A; V – скорость перебора паролей злоумышленником; T – максимальный срок действия пароля.

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

$$P = (V \cdot T) / S = (V \cdot T) / A^L. \quad (1)$$

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

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

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

$$S^* = [V \cdot P / T], \quad (2)$$

где [] – целая часть числа, взятая с округлением вверх.

После определения нижней границы S^* необходимо выбрать такие A и L для формирования $S = A^L$, чтобы выполнялось следующее неравенство:

$$S^* \le S = A^L. \quad (3)$$

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

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

Пример. Исходные данные: $P = 10^{-6}$; $T = 7$ дней = 1 неделя; $V = 10$ (паролей / минуту) = 10 · 60·24·7 = 100800 паролей в неделю. Тогда, $S^* = [(10800 \cdot 1) / 10^{-6}] = = 108 \cdot 10^8$.

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

Задание для выполнения лабораторной работы:

1) В таблице 3 найти для указанного варианта значения характеристик *P, V, T*.

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

3) Выбрать некоторый алфавит с мощностью A и получить минимальную длину пароля L, при котором выполняется условие (2).

4) Реализовать программу для генерации паролей пользователей. Программа должна формировать случайную последовательность символов длины L, при этом должен использоваться алфавит из A символов.

5) Оформить отчет по лабораторной работе.

Коды символов:

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

2) Коды цифр: «0» = 48,.., «9» = 57.

3) «!» = 33; «“» = 34; «#» = 35; «$» = 36; «%» = 37; «&» = 38; «‘» = 39.

4) Коды русских символов: «А» – 128, .,«Я» – 159; «а» – 160,…, «я» – 239.

Таблица 1- Варианты заданий

Вариант	*P*	*V*	*T*
1	10^{-4}	15 паролей/мин	2 недели
2	10^{-5}	3 паролей/мин	10 дней
3	10^{-6}	10 паролей/мин	5 дней
4	10^{-7}	11 паролей/мин	6 дней
5	10^{-4}	100 паролей/день	12 дней
6	10^{-5}	10 паролей/день	1 месяц
7	10^{-6}	20 паролей/мин	3 недели
8	10^{-7}	15 паролей/мин	20 дней
9	10-4	3 паролей/мин	15 дней

Окончание таблицы 1

10	10^{-5}	10 паролей/мин	1 неделя
11	10^{-6}	11 паролей/мин	2 недели
12	10^{-7}	100 паролей/день	10 дней
13	10^{-4}	10 паролей/день	5 дней
14	10^{-5}	20 паролей/мин	6 дней
15	10^{-6}	15 паролей/мин	12 дней
16	10^{-7}	3 паролей/мин	1 месяц
17	10^{-4}	10 паролей/мин	3 недели
18	10^{-5}	11 паролей/мин	20 дней
19	10^{-6}	100 паролей/день	15 дней
20	10^{-7}	10 паролей/день	1 неделя
21	10^{-4}	20 паролей/мин	2 недели
22	10^{-5}	15 паролей/мин	10 дней
23	10^{-6}	3 паролей/мин	5 дней
24	10^{-7}	10 паролей/мин	6 дней
25	10^{-4}	11 паролей/мин	12 дней
26	10^{-5}	100 паролей/день	1 месяц
27	10^{-6}	10 паролей/день	3 недели
28	10^{-7}	20 паролей/мин	20 дней
29	10^{-4}	15 паролей/мин	15 дней
30	10^{-5}	3 паролей/мин	1 неделя

Контрольные вопросы

1. Чем определяется стойкость подсистемы идентификации и аутентификации?
2. Перечислить минимальные требования к выбору пароля.
3. Перечислить минимальные требования к подсистеме парольной аутентификации.
4. Как определить вероятность подбора пароля злоумышленником в течение срока его действия?
5. Выбором каких параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником при заданной скорости подбора пароля злоумышленником и заданном сроке действия пароля?

2 Лабораторная работа №2. Симметричные алгоритмы шифрования данных

Цель: освоение методики работы симметричных алгоритмов шифрования.

Теоретические сведения.

Необходимо написать программу, реализующую шифрование и дешифрование текстового файла, используя один из симметричных алгоритмов. Программа должна обеспечить ввод имен файлов входных и выходных данных, ввод ключа, шифрование исходного файла, дешифрование.

Задание для выполнения лабораторной работы:

1) Алгоритм DES.
2) Отечественный стандарт шифрования.
3) Синхронные потоковые алгоритмы.
4) Блочный алгоритм.
5) Алгоритмы перестановки.

Контрольные вопросы

1**.** Цель и задачи криптографии.
2. Симметричные криптосистемы: шифры перестановки.
3. Симметричные криптосистемы: шифры простой замены.
4. Симметричные криптосистемы: шифры сложной замены.
5. Симметричные криптосистемы: гаммирование.

3 Лабораторная работа №3. Асимметричные алгоритмы шифрования данных

Цель: освоение методики работы ассиметричных алгоритмов шифрования, где существует два ключа – один для шифрования, другой для дешифрования.

Теоретические сведения.

Алгоритм RSA разработан в 1977 г. Роном Ривестом, Ади Шамиром и Леном Адлеманом и опубликован в 1978 г. С тех пор алгоритм Rivest-Shamir-Adleman (RSA) широко применяется практически во всех приложениях, использующих криптографию с открытым ключом.

Алгоритм RSA:

1) Вычисление ключей.

Важным моментом в этом криптоалгоритме является создание пары ключей: открытого и закрытого. Для алгоритма RSA этап создания ключей состоит из следующих операций:

1) Выбираются два простых различных числа p и q. Вычисляется их произведение $n = p \cdot q$, называемое модулем. Под простым числом будем понимать такое число, которое делится только на 1 и на само себя. Взаимно простыми числами будем называть такие числа, которые не имеют ни одного общего делителя, кроме единицы.

2) Вычисляется функция Эйлера $\Phi(n) = (p - 1) \cdot (q - 1)$.

3) Выбирается произвольное число e (e <n) такое, что 1 <e <$\Phi(n)$, и не имеет общих делителей, кроме 1 (взаимно простое) с числом $(p - 1) \cdot (q - 1)$.

4) Вычисляется d методом Евклида таким образом, что $(e \cdot d - 1)$ делится на $(p - 1) \cdot (q - 1)$.

5) Два числа (e, n) публикуются как открытый ключ.

6) Число d хранится в секрете – закрытый ключ есть пара (d, n), который позволит читать все послания, зашифрованные с помощью пары чисел (e, n).

2) Шифрование.

Шифрование с помощью пары чисел производится следующим образом:

1) Отправитель разбивает своё сообщение M на блоки m_i. Значение m_i <n, поэтому длина блока m_i в битах не больше $k = [\log_2(n)]$ бит, где квадратные скобки обозначают, взятие целой части от дробного числа.

Например, если $n = 21$, то максимальная длина блока $k = [\log_2(21)] = [4.39\ldots] = = 4$ бита.

2) Подобный блок может быть интерпретирован как число из диапазона $(0; 2^k - 1)$. Для каждого такого числа m_i вычисляется выражение (c_i – зашифрованное сообщение): $c_i = ((m_i)^e) \bmod n$.

Необходимо добавлять нулевые биты слева в двоичное представление блока c_i до размера $k = [\log_2(n)]$ бит.

3) Дешифрование.

Чтобы получить открытый текст, необходимо каждый блок дешифровать отдельно: mi = $((c_i)^d) \bmod n$.

Пример:

Выбрать два простых числа: $p = 7$, $q = 17$. Вычислить $n = p \cdot q = 7 \cdot 17 = 119$. Вычислить $\Phi(n) = (p - 1) \cdot (q - 1) = 96$.

Выбрать e так, чтобы e было взаимно простым с $\Phi(n) = 96$ и меньше, чем $\Phi(n)$: $e = 5$.

Определить d так, чтобы $d \cdot e \equiv 1 \bmod 96$ и $d < 96$, $d = 77$, так как $77 \cdot 5 = 385 = 4 \cdot 96 + 1$.

Результирующие ключи открытый {5, 119} и закрытый ключ {77, 119}.

Например, требуется зашифровать сообщение $M = 19$: $19^5 = 66 \pmod{119}$, $C = = 66$.

Для дешифрования вычисляется $66^{77} \pmod{119} = 19$.

Задание для выполнения лабораторной работы:

1) Разработать консольное приложение для шифрования/дешифрования произвольных файлов с помощью алгоритма RSA.

2) Разработать визуальное приложение для шифрования/дешифрования произвольных файлов.

4) Разработать клиент-серверное приложение для защищённой передачи файлов по сети.

5) Разработать клиент-серверное приложение для защищённого обмена сообщениями по сети.

6) Разработать визуальное приложение для шифрования/дешифрования чисел.

7) Разработать консольное приложение для генерации ключей.

8) Реализовать программу для шифрования / дешифрования текстов, работающую по алгоритму RSA. Программа должна уметь работать с текстом произвольной длины.

Контрольные вопросы

1. Дайте определение алгоритма с открытым ключом.
2. Сколько этапов содержит алгоритм RSA?
3. В чем заключается вычисление ключей алгоритма RSA?
4. Как происходит шифрование в алгоритме RSA?
5. Как происходит дешифрование в алгоритме RSA?

4 Лабораторная работа № 4. Антивирусная защита

Цель: знакомство с антивирусными программами и приобретение навыков работы с ними (проверка настроек антивирусов, сканирование файлов, папок и дисков, обновления антивирусной базы).

Теоретические сведения.

Компьютерный вирус– это вредоносная программа, которая самостоятельно может создавать свои копии и внедрять их в программы (исполняемые файлы), документы, загрузочные сектора носителей данных. В зависимости от среды обитания основными типами компьютерных вирусов являются: программные, загрузочные, макровирусы, сетевые вирусы.

Компьютерные вирусы были и остаются одной из наиболее распространенных причин потери информации. По данным Международной Ассоциации за безопасность компьютеров (International Computer Security Association- ICSA) количество компьютеров, страдающих от вирусных атак, растет с каждым годом. Убытки, наносимые компьютерными вирусами, составляют астрономические суммы.

Основным источником вирусов на сегодняшний день является глобальная сеть Интернет. Выделяют следующие точки проникновения вирусов в сеть:

- получение вирусов на клиентские рабочие места через носители;
- получение их на уровне файл-серверов;
- получение через интернет и почтовые шлюзы.

По выполняемым функциям антивирусные программы подразделяют на следующие типы: детекторы; доктора; ревизоры; фильтры или сторожа; вакцины или иммунизаторы.

Программы-ревизоры запоминают исходное состояние программ, каталогов и системных областей до заражения компьютера и периодически его сравнивают с текущим состоянием. При обнаружении несоответствия пользователю выдается предупреждение.

Программы-фильтры представляют собой резидентные программы, которые обеспечивают обнаружение подозрительных действий при работе компьютера, например, попыток изменения исполняемых файлов, изменения атрибутов файлов, записи в загрузочный сектор диска и др.

Программы-детекторы настроены на обнаружение заражения одним или несколькими известными вирусами. Большинство программ-детекторов выполняют также функцию «доктора», т.е. они пытаются вернуть зараженные файлы и области диска в исходное состояние, те файлы, которые не удалось восстановить, обычно делаются неработоспособными и удаляются.

Программы-доктора обнаруживают и лечат зараженные объекты путем «выкусывания» тела вируса. Программы этого типа подразделяются на фаги и полифаги (обнаружение и уничтожение большого количества разнообразных вирусов).

Программы-вакцины выполняют модификацию файла или диска таким образом, чтобы это не отражалось на их работе, но вирус считал бы их уже зараженными. Вакцинация осуществляется только от известных вирусов.

Антивирусные программы:

1) Kaspersky Internet Security.
2) Kaspersky CRYSTAL.
3) Касперский Яндекс-версия.
4) ESET NOD32 Антивирус.
5) ESET NOD32 Smart Security.
6) ESET NOD32 Titan.
7) Web Security Space.
8) Антивирус Dr.Web для Windows.
9) Avast Free Antivirus.
10) Avast Internet Security.
11) Panda Cloud Antivirus Free.
12) Norton AntiVirus 2013.
13) Avira Free Antivirus.
14) Microsoft Security Essentials.
15) AVG AntiVirus FREE 2014.
16) Ad-Aware Free Antivirus.

17) Comodo Antivirus 2013.

Задание для выполнения лабораторной работы:

1) Знакомство с Антивирусным обеспечением и утилитой согласно варианту, их письменное описание и ссылки для скачивания.
2) Проверьте дату и способы обновления антивирусных баз антивируса, способы настройки с пояснениями и скриншотами.
3) Выполните сканирование дисков (к примеру флэш) с пояснениями и скриншотами.
4) Выполните сканирование папок с файлами с пояснениями и скриншотами.

5 Запустите и опишите принцип работы заданной утилиты с пояснениями и скриншотами.

Предоставьте преподавателю результаты выполненной работы. Оформите отчет. В отчете должны присутствовать:

1) Краткое описание.
2) Принципы настройки, установки, обновления.
3) Примеры сканирования папки, диска, флэшки.
4) Пример работы утилиты.
5) Ссылки на страницы для скачивания антивирусного ПО и утилиты.

5 Лабораторная работа №5. Анализаторы протоколов

Цель: получить практические навыки в использовании анализаторов протоколов.

Теоретические сведения.

Анализатор трафика, или сниффер (от англ. to sniff — нюхать) — сетевой анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, предназначенного для других узлов.

Во время работы сниффера сетевой интерфейс переключается в т. н. режим прослушивания (Promiscuous mode), что и позволяет ему получать пакеты, адресованные другим интерфейсам в сети.

Перехват трафика может осуществляться:

- обычным прослушиванием сетевого интерфейса (метод эффективен при использовании в сегменте концентраторов (хабов) вместо коммутаторов (свитчей), в противном случае метод малоэффективен, поскольку на сниффер попадают лишь отдельные фреймы);
- подключением сниффера в разрыв канала;
- ответвлением (программным или аппаратным) трафика и направлением его копии на сниффер;
- через анализ побочных электромагнитных излучений и восстановление таким образом прослушиваемого трафика;

– через атаку на канальном (MAC-spoofing) или сетевом уровне (IP-spoofing), приводящую к перенаправлению трафика жертвы или всего трафика сегмента на сниффер с последующим возвращением трафика в надлежащий адрес.

В начале 1990-х широко применялся хакерами для захвата пользовательских логинов и паролей, которые в ряде сетевых протоколов передаются в незашифрованном или слабозашифрованном виде. Широкое распространение хабов позволяло захватывать трафик без больших усилий в больших сегментах сети практически без риска быть обнаруженным.

Снифферы применяются как в благих, так и в деструктивных целях. Анализ прошедшего через снифер трафика позволяет:

1) Обнаружить паразитный, вирусный и закольцованный трафик, наличие которого увеличивает загрузку сетевого оборудования и каналов связи.
2) Выявить в сети вредоносное и несанкционированное ПО, например, сетевые сканеры, флудеры, троянские программы, клиенты пиринговых сетей и другие (это обычно делают при помощи специализированных снифферов - мониторов сетевой активности).
3) Перехватить любой незашифрованный (а порой и зашифрованный) пользовательский трафик с целью получения паролей и другой информации.
4) Локализовать неисправность сети или ошибку конфигурации сетевых агентов (для этой цели снифферы часто применяются системными администраторами).

Поскольку в классическом сниффере анализ трафика происходит вручную, с применением лишь простейших средств автоматизации (анализ протоколов, восстановление TCP-потока), то он подходит для анализа лишь небольших его объёмов.

Снифферы для ОС MS Windows:

– CommView – www.tamos.com;
– SpyNet – packetstorm.securify.com;
– Analyzer – neworder.box.sk;
– IRIS – www.eeye.com;
– WinDUMP – аналог tcpdump for Unix;
– SniffitNT;
– ButtSniff;
– Wireshark;
– LanExplorer;
– Net Analyzer.
– IP Sniffer.

Снифферы для ОС Unix/Linux:

– Linsniffer;
– linux_sniffer;
– Sniffit;

- HUNT;
- READSMB;
- Tcpdump;
- Dsniff;
- Wireshark;
- Ksniffer.

Задание для выполнения лабораторной работы:

Используя программу Wireshark, выполните анализ трафика. В отчете представить результаты выполнения по всем пунктам в виде:

1) № задания.
2) Текст задания.
3) Результат работы программы.

Варианты заданий:

1) Изучить интерфейс программы Wireshark (\\corp.mgkit.ru\dfs\work\wireshark).
2) Захватить 100 произвольных пакетов. Определить статистические данные:
- процентное соотношение трафика разных протоколов в сети;
- среднюю скорость кадров/сек;
- среднюю скорость байт/сек;
- минимальный, максимальный и средний размеры пакета;
- степень использования полосы пропускания канала (загрузку сети).

3) Зафиксировать 20 IP-пакетов. Определить статистические данные: процентное соотношение трафика разных протоколов стека tcp/ip в сети; средний, минимальный, максимальный размеры пакета.
4) Выполнить анализ ARP-протокола по примеру из методических указаний.
5) На примере любого IP-пакета указать структуры протоколов Ethernet и IP, отметить поля заголовков и описать их.
6) Проанализировать и описать принцип работы утилиты ping.

При этом описать все протоколы, используемые утилитой. Описать все поля протоколов. Составить диаграмму взаимодействия машин при работе утилиты ping.

7) Режим захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10.
8) Режим перехвата только пакетов, отправленных на определенный IP-адрес. Количество захватываемых пакетов ограничить 5.
9) Режим перехвата только пакетов, полученных с определенного IP-адреса. Количество захватываемых пакетов ограничить 3.
10) Режим перехвата только пакетов протокола ICMP, отправленных на определенный IP-адрес. Количество захватываемых пакетов ограничить 3.

11) Режим захвата ARP-запроса с ПК студента на заданный преподавателем ПК и ARP-ответ на этот запрос. Количество захватываемых пакетов ограничить 2. Результат работы программы писать в файл.
12) Режим сохранения данных в двоичном режиме так, чтобы он перехватывал только пакеты, отправленные с ПК студента или пришедшие на него. Количество захватываемых пакетов ограничить.
13) Режим перехвата только пакетов, полученных с определенного IP-адреса. Количество захватываемых пакетов ограничить 4.
14) Режим перехвата только пакетов протокола ICMP, отправленных на определенный IP-адрес. Количество захватываемых пакетов ограничить 4.

Результат работы программы записать в файл.

Контрольные вопросы

1. Каковы основные цели мониторинга сетевого трафика?
2. Чем отличается мониторинг трафика от фильтрации?
3. Каково назначении класса программ-снифферов?
4. Какие основные функции выполняют снифферы?
5. Зачем используются фильтры отображения и фильтры захвата сниффера Wireshark? В чем их отличие?
6. Какие базовые функции статистической обработки захваченных пакетов имеет сниффер Wireshark?
7. Какие задачи рассчитан решать протокол ARP?

6 Лабораторная работа №6. Сбор информации о веб-приложении

Цель: обучение методам и средствам сбора информации об анализируемом веб-приложении.

Теоретические сведения.

Одним из первых этапов анализа защищенности любой компьютерной системы является сбор информации. В зависимости от используемой методологии анализа защищенности веб-приложения могут применяться различные методы и средства сбора информации. Стоит отметить, что сбор информации, как правило, не характерен для методологии инструментального анализа защищенности (сканирования), а характерен для методологии тестирования на возможность проникновения.

Методы сбора информации делятся на активные и пассивные. Активные методы требуют непосредственного взаимодействия с исследуемым приложением путем отправки ему запросов и анализа соответствующих ответов, а пассивные методы используют информацию, отправляемую сервером веб-приложения его клиентам (например, HTTP-заголовки X-Frame-Options, Strict-Transport-Security и т.д.) без отправки запросов. При анализе веб-приложений, как правило, используются только активные методы. Активные методы делятся на методы с подключением к приложению

(например, идентификация веб-сервера с помощью сканера Httprint) и методы без подключения (например, сбор информации о приложении поисковыми роботами, сканерами Интернет, и т.д.).

В результате проведения сбора информации о веб-приложении могут быть получены:

- имена и IP-адреса сетевых узлов, на которых размещены веб-приложение и его компоненты;
- логины и пароли технологических учетных записей;
- данные о системном и прикладном ПО, применяемых средств защиты и конфигурации веб-приложения;
- адреса электронной почты разработчиков приложения;
- исходный код серверной части веб-приложения;
- конфиденциальные файлы.

Программными средствами получения необходимой информации являются:

- поисковые системы (например, Google, Shodan, Bing);
- специализированные сканеры уязвимостей Интернет (например, http://un1c0rn.net/);
- инструментальные средства анализа защищенности сетей общего назначения (Nmap, Xprobe2, XSpider);
- инструментальные средства анализа защищенности сетей веб-приложений (AppScan, Acunetix, Burp Suite, ZAP, W3AF и т.д.).

Задание для выполнения лабораторной работы:

Выполнить сбор информации об анализируемом веб-приложении www.test.app.com.

Последовательность действий.

Будем рассматривать сбор информации на примере веб-приложения с условным именем www.test.app.com:

1) В адресной строке браузера перейти по адресу www.test.app.com/robots.txt. Проанализировать содержимое файла. Сделать выводы о наличии «скрытых» директорий.
2) В адресной строке браузера перейти по адресу http://www.test.app.com/crossdomain.xml и затем по адресу http://www.test.app.com/clientaccesspolicy.xml. Проанализировать содержимое файлов. Сделать выводы о корректности конфигурации политики междоменного взаимодействия RIA.
3) Перейти по адресу http://www.google.com. Задать поисковые запросы, определяемые анализируемым приложением, например:

- site:www.test.app.com filetype:docx confidential;
- site:www.test.app.com filetype:doc secret;
- site:www.test.app.com inurl:admin;

– site:www.test.app.com filetype:sql;
– site:www.test.app.com intext: "Access denied".

Проанализировать логику запросов и полученные данные. Построить свои запросы, используя примеры из базы запросов.

4) Перейти по адресу http://www.shodanhq.com. Используя бесплатную версию монитора сетевой безопасности (Monitor Network Security), задайте следующий поисковый запрос:

– hostname:www.test.app.com

Построить свои запросы для приложения www.test.app.com.

5) Данный тест выполняется только для приложений, размещенных в лабораторной сети. С помощью сетевых сканеров Nmap и Xprobe выполнить идентификацию ОС веб-сервера:

nmap –O www.test.app.com –vv

xprobe2 www.test.app.com

6) Подключиться к веб-серверу, используя утилиту Netcat:

nc www.test.app.com 80

Отправить следующий GET запрос:

GET / HTTP/1.1

Host: www.test.app.com \r\n

По заголовкам Server и X-Powered-By определить программное обеспечение, реализующее веб-сервер и фрэймворк веб-приложения.

В браузере установить расширение Wappalyzer, перейти по адресу веб-приложения и проанализировать информацию о компонентах веб-приложения, полученного через Wappalyzer.

7) С помощью сканера веб-серверов Httprint (дистрибутив Backtrack) или Httprecon (ОС Windows) выполнить идентификацию веб-сервера:

cd /pentest/enumeration/web/httprint/linux

./httprint –h www.test.app.com –s signatures.txt

С помощью сканера Wafw00f проверить наличие у веб-приложения подсистемы WAF:

cd /pentest/web/waffit

python ./wafw00f.py http://www.test.app.com

python ./wafw00f.py https://www.test.app.com

8) Выполнить тесты по идентификации поддерживаемых веб-сервером HTTP-методов. Для этого необходимо отправить с помощью Burp Suite или Netcat запрос следующего вида:

OPTIONS / HTTP/1.1

Host: www.test.app.com \r\n

Проверить, поддерживает ли сервер обработку запросов с произвольными методами:

DOGS / HTTP/1.1

Host: www.test.app.com \r\n

Если веб-сервер поддерживает метод TRACE, то это может привести к уязвимости к атаке Cross-Site Tracing (XST). Для проверки поддержки веб-сервером методы TRACE отправить запрос

TRACE / HTTP/1.1

Host: www.test.app.com \r\n

Веб-сервер поддерживает метод TRACE и потенциально уязвим к атаке XST, если получен ответа вида

HTTP/1.1 200 OK

Connection: close

Content-Length: 39

TRACE / HTTP/1.1

Host: www.test.app.com

Контрольные вопросы

1. Какую информацию вам дает анализ защищенности веб-приложений?
2. Перечислите активные методы сбора информации.
3. Перечислите пассивные методы сбора информации.
4. Какую уязвимость имеет метод TRACE?
5. Как лечат такую уязвимость?
6. Найти административные интерфейсы коммуникационного и сетевого оборудования (видеокамеры, коммутаторы ЛВС, домашние Wi-Fi маршрутизаторы, и т.д.), подключенные к сети Интернет.
7. Известно, что адрес веб-интерфейса системы VMWare Horizon View HTML Access содержит строку portal/webclient/views/mainUI.html.

   Найти такие системы, доступные из сети Интернет.
8. Оценить количество коммутаторов Cisco Catalyst с административным веб-интерфейсом, подключенным к сети Интернет.

7 Лабораторная работа №7. Защита от копирования. Привязка к аппаратному обеспечению. Использование реестра

Цель: ознакомление с возможностями «привязки» к характеристикам компьютера.

Теоретические сведения.

В качестве анализируемых характеристик компьютера могут использоваться:

1) Информация об используемой операционной системе.
2) Имя пользователя.
3) Имя компьютера.
4) Наличие звуковой карты.
5) Наличие подключенных принтера, сканера и т.д.

6) Дата создания BIOS.

7) Серийный номер диска.

8) Характеристики процессора.

Для получения подобных характеристик в операционной системе Windows используются API-функции и информация из реестра.

API-функции.

API сокращено от Application Programming Interface (интерфейс прикладного программирования). API – набор функций, которые операционная система предоставляет программисту. API обеспечивает относительно простой путь для программистов при использовании полных функциональных возможностей аппаратных средств или операционной системы.

32-разрядные версии Windows обычно используют один и тот же набор функций API, хотя имеются некоторые различия между платформами.

Почти все функции, которые составляют Windows API, находятся внутри DLL (Dynamic Link Library). Эти dll-файлы находятся в системной папке Windows. Существует свыше 1000 функций API, которые условно делятся на четыре основные категории:

а) работа с приложениями – запуск и закрытие приложений, обработка команд меню, перемещения и изменения размера окон;

б) графика – создание изображений;

в) системная информация – определение текущего диска, объема памяти, имя текущего пользователя и т.д.

г) работа с реестром – манипуляции с реестром Windows.

Реестр Windows.

Реестр – база данных операционной системы, содержащая конфигурационные сведения. По замыслу Microsoft, реестр должен был полностью заменить файлы ini, которые были оставлены только для совместимости со старыми программами, ориентированными на более ранние версии операционной системы.

Переход от ini файлов к реестру произошел по той причине, что на эти файлы накладывается ряд серьезных ограничений, и главное из них состоит в том, что предельный размер такого файла составляет 64Кб.

Предупреждение: никогда не удаляйте или не меняйте информацию в реестре, если Вы не уверены, что это именно то, что нужно. В противном случае некорректное изменение данных может привести к сбоям в работе Windows, и, в лучшем случае, информацию придется восстанавливать из резервной копии.

Реестр имеет следующую структуру:

1) HKEY_CLASSES_ROOT. В этом разделе содержится информация о зарегистрированных в Windows типах файлов, что позволяет открывать их по двойному щелчку мыши, а также информация для OLE и операций drag-and-drop.

2) HKEY_CURRENT_USER. Здесь содержатся настройки оболочки пользователя (например, Рабочего стола, меню "Пуск", ...), вошедшего в Windows. Они дублируют содержимое подраздела HKEY_USER\name, где name – имя пользователя, вошедшего в Windows. Если на компьютере работает один пользователь и используется обычный вход в Windows, то значения раздела берутся из подраздела HKEY_USERS\.DEFAULT.

3) HKEY_LOCAL_MACHINE. Этот раздел содержит информацию, относящуюся к компьютеру: драйверы, установленное программное обеспечение и его настройки.

4) HKEY_USERS. Содержит настройки оболочки Windows для всех пользователей. Как было сказано выше, именно из этого раздела информация копируется в раздел HKEY_CURRENT_USER. Все изменения в HKCU (сокращенное название раздела HKEY_CURRENT_USER) автоматически переносятся в HKU.

5) HKEY_CURRENT_CONFIG. В этом разделе содержится информация о конфигурации устройств Plug&Play и сведения о конфигурации компьютера с переменным составом аппаратных средств.

6) HKEY_DYN_DATA. Здесь хранятся динамические данные о состоянии различных устройств, установленных на компьютере пользователя. Именно сведения этой ветви отображаются в окне «Свойства: Система» на вкладке «Устройства», вызываемого из Панели управления. Данные этого раздела изменяются самой операционной системой, так что редактировать что-либо вручную не рекомендуется.

Примеры процедур и функций, определяющих параметры компьютера.

Определение серийного номера раздела диска.

```
TCHAR    szVolName[256];
DWORD    dwNum;
DWORD    dwMaxComSize;
DWORD    dwFlags;
TCHAR    szFS[256];
BOOL     bRes;
bRes = GetVolumeInformation ( "c:\\", szVolName, sizeof(szVolName),
&dwNum, &dwMaxComSize, &dwFlags, szFS, sizeof(szFS));
```

Определение имени компьютера.

```
const int WSVer = 0x101;
WSADATA wsaData;
char Buf[128];
if (WSAStartup(WSVer, &wsaData) == 0)
{
  gethostname(&Buf[0], 128);
  MessageBox(0, Buf,0,0);
  WSACleanup;
}
```

Определение имени пользователя.

```
char buffer[UNLEN+1];
DWORD size;
size=sizeof(buffer);
GetUserName(buffer,&size);
```

Определение частоты процессора (способ №1).

```
double CPUSpeed(void)
  {
```

```
  DWORD dwTimerHi, dwTimerLo;
  asm
   {
      DW 0x310F
      mov dwTimerLo, EAX
      mov dwTimerHi, EDX
    }
  Sleep (500);
  asm
   {
      DW 0x310F
      sub EAX, dwTimerLo
      sub EDX, dwTimerHi
      mov dwTimerLo, EAX
      mov dwTimerHi, EDX
   }
  return dwTimerLo/(1000.0*500);
}
```

Задание для выполнения лабораторной работы:

Разработать программу, реализующую привязку к компьютеру, используя совокупность характеристик согласно варианту задания. Добиться того, чтобы программа не запускалась на другом компьютере.

Таблица 2- Варианты заданий

№ варианта	Характеристики
1	Серийный номер раздела жесткого диска, MAC-адрес сетевой карты
2	Информация из реестра, тактовая частота процессора
3	Версия операционной системы, MAC-адрес сетевой карты
4	Имя пользователя, серийный номер раздела жесткого диска
5	Название компьютера, информация из реестра
6	Версия БИОС, имя пользователя
7	Серийный номер раздела жесткого диска, имя пользователя
8	Имя пользователя, тактовая частота процессора
9	MAC-адрес сетевой карты, тактовая частота процессора

Контрольные вопросы

1. Что понимается под «привязкой» к компьютеру?
2. Какие характеристики обычно используются для идентификации компьютера?
3. Перечислите основные API-функции для определения индивидуальных характеристик компьютера.
4. Что представляет собой реестр Windows?
5. Какую структуру имеет реестр?
6. Как определить серийный номер диска?
7. Как определить имя компьютера?

8 Лабораторная работа № 8. Обеспечение безопасности компьютерной системы

Цель: знакомство с методами защиты от вторжений, навыками настройки брандмауэров, средствами защиты от спама и вредоносных программ и вирусов.

Теоретические сведения.

1. Защита от вторжений. Брандмауэры.

Атаки на операционные системы, важнейшая проблема обеспечение безопасности компьютера.

Поскольку взаимодействие компьютера с внешним миром осуществляется через порты, а их достаточно много (65536 в IBM-совместимом компьютере), то целесообразна идея закрытия большинства из них, кроме немногих (одного-двух), абсолютно необходимых. Определить, насколько компьютер открыт для внешнего мира, можно с помощью специальных тестов, позволяющих оценить уровень уязвимости компьютера. Следующие сайты могут помочь в решении этой задачи:

1) Symantec Security Check (http://security.symantec.com).
2) Sygate Online Services (http://users.telenet.be/visvoer/audit/disndag %20linux/scanudpsygate.html).
3) Gipson Research Shields Up (www.grc.com).
4) DSL Reports (www.dslreports.com/scan).

Для проверки компьютера нужно зайти на один из этих сайтов и выполнить представленные там инструкции.

Идеальных операционных систем не существует, в их числе и Windows XP. Поэтому Microsoft выпускает ежемесячные обновления безопасности, а также срочные внеплановые обновления. Веб-сайт Windows Update позволяет познакомиться со всеми критически важными обновлениями (critical update) и обновлениями механизмов операционной системы (features updates). Критически важные обновления призваны решать проблемы, связанные с безопасностью, например, проблему защиты от широко распространенного эксплойта для Windows XP, известного под именем червя W32. Blaster.Worm. Этот червь распространялся через уязвимость в системе RPC (вызов удаленных процедур).

В Windows XP имеется полезная служба автоматического обновления: установив расписание для ежедневной автоматической проверки и установки новых обновлений, можно отказаться от интерактивных посещений веб-сайта Windows Update. Для настройки параметров автоматического обновления нужно щелкнуть правой кнопкой мыши по значку *Мой компьютер* и выбрать в контекстном меню строку *Свойства*, а затем перейти на вкладку *Автоматическое обновление*.

Установив открытые порты компьютера, как это рассмотрено выше, можно их заблокировать, оставив минимальное количество открытых, с

помощью специальной программы - *брандмауэра*. Когда удаленный компьютер попытается через заблокированный порт получить доступ к компьютеру, на котором установлен брандмауэр, он не сможет этого сделать, потому что посылаемые удаленным компьютером данные будут игнорироваться.

При попадании данных в заблокированный порт в зависимости от настройки брандмауэр отвечает, что порт закрыт, или вообще ничего не отвечает, делая компьютер невидимым извне. Компьютер, на котором установлен брандмауэр, работающий в режиме невидимости, для любого удаленного компьютера, пытающегося к нему подключиться, будет выглядеть как выключенный, т.к. никакого ответа удаленный компьютер не получит.

В Windows XP имеется встроенный брандмауэр Internet Connection Firewall (ICF). Новая версия брандмауэра, являющаяся частью пакета обновлений Service Pack 2, имеет ряд новых возможностей, упрощающих работу с брандмауэром и обеспечивающих высокий уровень безопасности.

Брандмауэр по умолчанию отключен. Для его использования нужно выполнить следующие действия:

1) В главном меню выбрать команду *Выполнить*, затем в поле ввода открывшегося окна набрать строку firewall.cpl и щелкнуть по кнопке *ОК*.
2) После открытия диалогового окна установить переключатель *Включить* и щелкнуть по кнопке *ОК*.

По умолчанию, брандмауэр блокирует все подключения, поэтому его нужно настроить, чтобы трафик определенных приложений мог проходить через брандмауэр, Настройка заключается в указании программ, трафик которых не должен блокироваться брандмауэром. Для открытия брандмауэра для определенного приложения нужно выполнить следующие шаги:

1) Перейти на вкладку *Исключения*.
2) Просмотреть список всех разрешенных программ (слева от названий таких программ установлен флажок). Целесообразно сбросить флажки для всех программ, которые не предполагается использовать.
3) Если нужно добавить в список исключений новое приложение, которое должно обрабатывать подключения и данные из внешнего мира, следует щелкнуть по кнопке *Добавить программу*.
4) Из предложенного списка программ выделить название программы, щелкнуть по кнопке *ОК*, после чего название программы появится в списке.
5) Установить флажок возле имени добавленного приложения и щелкнуть *ОК* для активизации новых параметров брандмауэра.

Брандмауэр Windows позволяет задать режим ответа компьютера в случае посылки ему некоторых стандартных управляющих интернет-сообщений. Например, можно разрешить или запретить команду ping, которая используется для оценки интервала времени между посылкой данных какому-либо компьютеру и получением от него ответа. Для изменения соответствующего параметра нужно перейти на вкладку *Дополнительно* и щелкнуть по кнопке *Параметры* в разделе *Протокол* ICMP. Откроется

диалоговое окно *Параметры* ICMP. Если требуется, чтобы компьютер был невидим в Интернете, нужно сбросить все флажки в данном окне.

Брандмауэр Windows XP относится к брандмауэрам одностороннего типа, т.е. может блокировать только входящий трафик. Компания Zone Labs разработала двухсторонний брандмауэр ZoneAlarm, который поставляется в двух вариантах: профессиональная версия и бесплатная версия (базовый вариант двухстороннего брандмауэра), которую можно загрузить с сайта (www.zonealarm.com). Двухсторонний брандмауэр может блокировать не только входящий, но и исходящий трафик, который пытаются отослать приложения с компьютера пользователя.

Блокировать исходящий трафик может понадобиться по следующим причинам. Пользователь заботится о своей конфиденциальности и не желает, чтобы приложения, установленные на компьютере, связывались с веб-сайтом разработчика для пересылки туда данных, проверки обновлений или лицензий. Пользователю необходим контроль за тем, какие приложения получают доступ к Интернету. Пользователю необходима защита от программ подобных троянским коням. Двухсторонние брандмауэры типа ZoneAlarm делают подобные приложения бесполезными, т.к. подобные вредоносные программы оказываются изолированными и не могут связаться с Интернетом.

Для установки, настройки и запуска ZoneAlarm нужно выполнить следующие действия:

1) Загрузить копию программы с сайта www.zonealarm.com.
2) Выполнить инструкции мастера Configuration Wizard для настройки политики компьютера и запустить программу.
3) Установить режим работы брандмауэра. Такой режим устанавливается:

– для зоны Интернета (защита от незнакомых компьютеров). Для временной работы в зоне Интернета рекомендуется средний уровень защиты, при котором другие компьютеры могут видеть защищаемый компьютер, но не могут использовать его ресурсы;
– для зоны надежных узлов Интернета (зона доверия), в которой предполагается совместная работа с компьютерами. Рекомендуется средний уровень защиты, при котором другие компьютеры могут видеть защищаемый компьютер и могут использовать его ресурсы;
– для зоны блокированных узлов, через которые соединения запрещены. В эту зону включаются компьютеры, к которым нет доверительного отношения.

4) Если требуется настроить параметры блокировки приложений, нужно щелкнуть по ссылке *Program Control*, а затем на вкладке *Main* задать желаемый уровень контроля. Более детальный уровень контроля по каждому приложению можно задать на вкладке *Programs*. По умолчанию, некоторые программы (например, Internet Explorer) всегда имеют доступ в Интернет. Однако при первом запуске программы, которой требуется выход в Интернет (например, Windows Messenger), ZoneAlarm спросит (Ask), действительно ли

нужно пропустить трафик этого приложения. Нажав кнопку *Option*, можно получить сведения о выбранной программе.

Если ничего не известно о программе, запрашивающей доступ в Интернет, нужно поискать в Интернете информацию об этой программе. Возможно, что такой информации не будет найдено. В этом случае будет сделан вывод, что это - spyware- программа, которую нужно удалить.

5) В список программ, трафик которых пропускается через брандмауэр, можно добавить нужные элементы, щелкнув по кнопке Add.

2. Отключение ненужных служб.

С целью повышения защищенности компьютера некоторые службы можно отключить:

1) *Запрет на подключение удаленного рабочего стола*. Удаленный рабочий стол в Windows XP - это компонент операционной системы, позволяющий получить доступ к своему компьютеру в те моменты, когда пользователь находится вдали от своего офиса или дома. Если компьютер недостаточно хорошо защищен, удаленный рабочий стол может стать средством проникновения на компьютер. Вся защита удаленного рабочего стола основывается на пароле, который во многих случаях несложно подобрать. В связи с этим, если удаленный рабочий стол не используется, его лучше отключить. Для этого нужно сделать следующее:

- щелкнуть правой кнопкой мыши по значку *Мой компьютер* и выбрать в контекстном меню команду *Свойства*;
- в открывшемся окне перейти на вкладку *Удаленные сеансы*, позволяющую задать параметры удаленного доступа;
- сбросить флажки в разделах *Удаленный помощник* и *Дистанционное управление рабочим столом*. Щелкнуть по кнопке *ОК* для сохранения изменений.

2) *Отключение службы сообщений*. В последних версиях Windows имеется служба, позволяющая системному администратору посылать сообщения всем компьютерам в локальной сети. Это отличная служба, если ее использовать правильно. Некоторые пользователи, знающие про эту службу, могут злоупотреблять ею, рассылая сообщения и, хуже того, спам всем пользователям сети.

Служба сообщений, как и любая другая программа, имеющая доступ во внешнюю сеть, является потенциальной угрозой безопасности компьютера. Поэтому из соображений безопасности службу сообщений лучше отключить. Для этого выполнить команды: *Пуск* - *Программы* - *Администрирование* - *Службы*. В открывшемся окне *Службы* выбрать из списка служб строку *Служба сообщений*, щелкнуть по ней правой клавишей мыши и выбрать в контекстном меню команду *Свойства*. Далее в раскрывающемся списке *Тип запуска* выбрать пункт *Отключено* и щелкнуть по кнопке ОК для сохранения изменений.

3) *Отключение поддержки универсальной технологии Plug-and-Play*. Универсальная технология Universal Plug-and-Play (UPnP) представляет собой развитие технологии Plug-and-Play. Она позволяет быстро и просто добавлять и контролировать самые различные устройства. Учитывая низкую в настоящее время распространенность устройств UPnP и факт снижения уровня безопасности при использовании службы поддержки таких устройств, ее лучше отключить. Для этого нужно поступить так же, как и при отключении службы сообщений, но выбрать в перечне служб *Узел универсальных PnP-устройств*.

4) *Отключение удаленного доступа к реестру*. В состав Windows XP Professional входит служба *Удаленный реестр*, позволяющая пользователям с правами администратора подключаться к реестру компьютера и редактировать его. Чтобы не дать кому-либо дополнительный шанс проникнуть в один из наиболее важных компонентов операционной системы, лучше отключить эту службу.

5) *Отключение поддержки DCOM*. Поддерживаемая Windows технология DCOM (Distributed Component Object Model - распределенная объектная модель программных компонентов) предоставляет удобный интерфейс программирования для разработчиков сетевых приложений. Эксплойты, построенные на базе уязвимости DCOM, позволили распространиться интернет-червю по сотням тысяч машин с операционной системой Windows. Большинству пользователей можно отключить эту службу (исключение составляют лишь те пользователи, которые пользуются приложениями, реально требующими поддержки DCOM).

Компания Gibson Research разработала утилиту DCOMbobulator, которая поможет отключить DCOM на компьютере. Утилиту можно загрузить с сайта www.grc.com/dcom/. После ее запуска открывается окно, в котором нужно перейти на вкладку DCOMbobulator Me! и щелкнуть по кнопке Disable DCOM, а затем по кнопке Exit.

6) После установки всех настроек щелкнуть по кнопке Finish.

3. Защита от спама.

Наиболее распространенной причиной получения спама являются сами пользователи. Они посылают электронные сообщения на веб-сайты или в компании, которые в ответ рассылают им свою рекламу или продают их адреса другим компаниям, еще одна распространенная причина получения спама - невнимательная подписка на различные новости и информационные рассылки.

Так как программ для рассылки спама создано огромное количество, то не существует программы, которая фильтрует спам с гарантией 100%. Однако, если утилита будет отсекать около 90% нежелательной корреспонденции, это будет хорошим результатом. Одной из неплохих утилит является McAfee SpamKiller - программа для защиты от спама с ежедневным автообновлением базы по спамерам и легким созданием собственных фильтров.

Работает SpamKiller в фоновом режиме, проверяет практически неограниченное число почтовых ящиков, выявляет полученный спам и удаляет его прямо на почтовом сервере - автоматически или в ручном режиме. В случае обнаружения новой почты возможна разнообразная сигнализация об этом, а также автоматический запуск почтовой программы.

Условно-бесплатный вариант программы имеется на множестве сайтов Интернета, например, на сайте dl.softportal.com/load/spamkiller2908.exe. После загрузки и запуска программы открывается окно для инсталляции утилиты. Установленная утилита после ее запуска предлагает купить лицензионную версию или продолжить работу с 30-дневной демо- версией.

Нажав кнопку *Continue*, пользователь перейдет к мастеру установки параметров программы. После завершения работы с мастером настройки программы и нажатия кнопки *Finish* открывается окно программы, в котором можно просмотреть и установить параметры утилиты для фильтрации сообщений, в том числе поступающих из разных стран.

Если почтовый клиент пользователя поддерживает графические сообщения в формате HTML, то при каждом получении почты имеется вероятность того, что отправитель узнает, прочитал ли получатель его письмо. Это делается при помощи скрытых ссылок на изображения, обращающиеся к веб-серверу, на котором запущена специальная программа, отслеживающая подобные обращения. Если задержать сигналы, отправляемые на серверы распространителей спама, то, возможно, что адрес получателя будет удален из баз данных серверов как неактивный.

Последние версии некоторых почтовых программ, например, Outlook 2003 и Outlook Express (после установки Windows XP Service Pack 2), автоматически блокируют все внешние ссылки в HTML-сообщениях. Режим блокировки внешних ссылок в Outlook Express можно включить на вкладке *Безопасность* в окне *Параметры*, вызываемого из меню *Сервис*. В *Outlook* и *Outlook Express* также имеется список надежных отправителей, с помощью которого можно включать внешнее содержимое только для определенных отправителей. Чтобы разрешить использование рисунков и другого внешнего содержимого для определенного отправителя, нужно щелкнуть правой кнопкой мыши по сообщению от него и добавить отправителя в список надежных отправителей.

4. Защита от вредоносных программ и вирусов.

В последнее время spyware-программы превратились в наиболее опасную угрозу для компьютеров. Скрываясь в свободно распространяемых приложениях, эти программы шпионят за пользователями компьютеров и затем отправляют собранную информацию злоумышленникам. Шпионское ПО, не проявляя себя, отслеживает поведение пользователя за компьютером, чтобы создать его «маркетинговый профиль», который также молча передается сборщикам информации, продающим данные пользователя рекламным организациям.

Существует еще один вид вредоносных программ - adware-программы, тесно связанные со spyware-программами. Они также тайно устанавливаются на компьютеры пользователей и начинают наблюдать за ними. Обычно подобные ситуации связаны с установкой программ, загружаемых с веб-сайтов. Пользователи часто перед установкой бесплатных программ не читают соответствующие соглашения о предоставлении услуг и пропускают сообщения, что данные программы будут отображать рекламу.

Если в браузере появятся новые панели инструментов, которые явно не устанавливались, если браузер постоянно «падает» или стартовая страница неожиданно изменилась, то вполне вероятно, что в компьютере завелся «шпион». Но даже если нет ничего необычного, то «шпионы» все равно могут быть - чем дальше, тем больше появляется программное обеспечение такого рода.

В Интернете имеется множество свободно распространяемых утилит, помогающих проверить компьютер на наличие spyware и adware-программ. Наибольшей популярностью пользуются две такие программы. Первая программа Ad-ware разработана компанией Lavasoft, ее базовую версию можно загрузить бесплатно с сайта www.lavasoft.de. Вторая программа называется Spybot S&D и распространяется также бесплатно (www.spybot.info).

Для загрузки и запуска программы Ad-ware нужно выполнить следующее:

1) Загрузить копию базовой версии программы Ad-ware с сайта www.lavasoft.de и установить ее на компьютере.
2) Запустить программу – откроется окно.
3) Обновить файлы данных, щелкнув по кнопке *Web Update*, а затем *Update*. Если имеются актуальные обновления, будет выдано соответствующее сообщение. В этом случае щелкнуть по кнопке *Yes*, а затем- *OK*, после чего обновления будут автоматически загружены и установлены.
4) Для начала проверки компьютера щелкнуть по кнопке *Scan*. Из показанных режимов сканирования *Scan Mode* выбрать необходимый (например, Smart Scan) и нажать кнопку *Scan*. Начнется процесс сканирования.
5) После завершения сканирования будут показаны его результаты с перечислением всех spyware- и adware-программ, обнаруженных на компьютере. Нужно сбросить флажки у тех объектов, которые решено не удалять (например, у объектов типа Tracking cookie). Для удаления объектов нажать кнопку Remove. Программа автоматически сохраняет резервные копии всех удаляемых объектов на случай возникновения проблем в операционной системе после удаления файлов и параметров реестра.
6) Для завершения работы с программой нажать кнопку *Finish*.

Еще одна популярная программа Spybot - Search & Destroy (спайбот - найти и уничтожить) может обнаруживать и удалять с компьютера различного

рода шпионское программное обеспечение. Программу Spybot-S&D в русскоязычном варианте можно загрузить с сайта www.spybot.info.

После загрузки, инсталляции и запуска программы открывается ее окно с подменю Spybot-S&D. При первом запуске нужно прочитать несколько соглашений об ответственности за использование программы.

Далее для работы с программой нужно выполнить следующие действия:

1) Обновить файлы данных, для чего щелкнуть по кнопке *Поиск обновлений*. Просмотрев список доступных обновлений, для их загрузки щелкнуть по кнопке *Загрузить обновления*.
2) После загрузки и установки обновлений нужно закрыть и заново открыть программу. Для проверки компьютера нажать кнопку *Начать проверку*. Начнется процесс сканирования.
3) Результаты сканирования будут через некоторое время выведены в окне результатов.
4) Для устранения выявленных проблем нужно нажать клавишу *Устранить отмеченные проблемы*. Устранению подлежат только те файлы, которые помечены флажками. Программа автоматически сохраняет резервные копии всех удаляемых объектов на случай возникновения проблем в операционной системе после удаления файлов и параметров реестра.
5) Перед устранением выявленных проблем программа создает резервную копию реестра. Если возникнут какие-либо трудности с операционной системой, можно восстановить удаленные файлы и исходное состояние реестра. Для этого нужно щелкнуть по клавише *Восстановить*. Предварительно программа предложит создать резервную копию реестра.

С помощью утилиты Spybot-S&D можно выполнять вакцинацию, защищающую компьютер от некоторых наиболее распространенных типов вредоносных программ. Данная возможность значительно повышает защищенность компьютера в борьбе с spyware-программами. Для выполнения вакцинации нужно запустить утилиту и щелкнуть по кнопке *Иммунизация*.

После удаления с компьютера всех spyware- и adware-программ можно отключить некоторые режимы работы браузера Internet Explorer, снизив тем самым риск новой случайной установки spyware-программ.

Целесообразно изменить параметры установки элементов ActiveX, запретив возможность их установки. Для этого необходимо выполнить следующие действия:

1) Открыть новое окно Internet Explorer.
2) Выбрать команду *Свойства обозревателя* в меню *Сервис*.
3) Перейти на вкладку *Безопасность* и щелкнуть по кнопке *Другой*. Откроется окно *Параметры безопасности*.
4) Найти в списке группу переключателей *Загрузка подписанных элементов ActiveX* и установить переключатель в состояние *Отключить* (загрузка неподписанных элементов также должна быть отключена).
5) Щелкнуть по кнопке *ОК*, а затем - по кнопке *Да*.

6) Еще раз щелкнуть по кнопке *ОК* для закрытия окна *Свойства обозревателя*.

Выполненная процедура приведет к запрету установки элементов управления ActiveX с любых веб-сайтов (как хороших, так и плохих). Если при посещении какого-либо сайта возникнут проблемы с загрузкой его содержимого, то можно выполнить обратную процедуру, т.е. разрешить загрузку подписанных элементов ActiveX.

5. Защита конфиденциальной информации.

Современные операционные системы, в том числе Windows XP, собирают много информации о работе пользователя за компьютером. Сюда относятся адреса веб-сайтов, имена запускаемых приложений и открываемых файлов. Эта информация используется системой для обеспечения комфортной работы пользователя. Однако иногда это нежелательно, например, если необходимо соблюдать конфиденциальность своей работы. Это особенно актуально, если компьютером пользуется несколько человек. Для соблюдения конфиденциальности своей работы информацию о действиях пользователя необходимо с компьютера удалить.

Очистка Internet Explorer. В целях конфиденциальности приходится очищать четыре части данных браузера: список вводившихся адресов, журнал с историей посещения веб-сайтов, список временных файлов Интернета и список cokie-файлов. Первый список формируется на основе истории ранее вводившихся адресов и позволяет быстро вводить адреса, выбирая их среди возможных вариантов. Отключить функцию автоматического завершения ввода довольно непросто. Файл, в котором хранится это список, является URL-кэшем и имеет имя index.dat. Решение можно получить с помощью утилиты Dr.Delete (http://www.docsdownloads.com/dr-delete-1.htm), для этого нужно выполнить следующие шаги:

1) Запустить программу Dr. Delete и щелкнуть по кнопке *Browse*, чтобы выбрать удаляемый файл.
2) Открыть папку C:\documents and Settings.
3) Открыть папку, название которой совпадает с вашим именем пользователя.
4) Открыть папку Cookies, выделить файл index.dat и щелкнуть по кнопке *Open*.
5) После того как в поле ввода появится путь к файлу, щелкнуть по кнопке *Delete*.
6) Щелкнуть по кнопке *Yes* в диалоговом окне подтверждения. Появится сообщение о том, что данный файл будет удален при следующей перезагрузке компьютера.

По умолчанию, Internet Explorer настроен на запись адресов веб-сайтов, которые посещались в течение 30 дней. Если важно сохранить конфиденциальность этих посещений, нужно периодически очищать журнал посещений. Для очистки журнала посещений нужно выполнить следующие действия:

1) Открыть окно браузера Internet Explorer и в меню *Сервис* выбрать команду *Свойства*. Откроется окно *Свойства*: *Интернет*.
2) На вкладке *Общие* щелкнуть по кнопке *Очистить*. Появится диалоговое окно *Свойства обозревателя*, в котором нажать кнопку *Да*.
3) Указать интервал времени, в течение которого должна храниться информация о посещении сайтов. Щелкнуть по кнопке *Применить* и *ОК*.

Каждый раз при посещении сайтов Интернета в компьютере в папку Temporary Internet Files записываются соответствующие файлы. Со временем папка вырастает в объеме и может содержать информацию, которую нежелательно показывать другим пользователям этого компьютера. Однако папка доступна для просмотра каждому пользователю. Если это нежелательно, папку Temporary Internet Files следует очистить.

Еще один вид файлов, которые создаются при посещении Интернета, - Cookie-файлы. С точки зрения конфиденциальности, единственный минус хранения этих файлов на компьютере связан с тем, что он доступен локальным пользователям этого компьютера. Следовательно, при желании они могут определить, какие сайты кто посещал. Для очистки папки Temporary Internet Files и удаления Cookie-файлов нужно выполнить следующие действия:

1) Открыть новое окно браузера Internet Explorer и в меню *Сервис* выбрать команду *Свойства обозревателя*.
2) Щелкнуть по кнопке *Удалить файлы* в разделе *Временные файлы Интернета*. Появится запрос, в котором нужно установить флажок и щелкнуть по кнопке *ОК*.
3) После возврата в окно *Свойства обозревателя* нужно щелкнуть по кнопке *Удалить* «Cookie».
4) Щелкнуть по кнопке *ОК* в диалоговом окне подтверждения и еще раз *ОК* для закрытия окна *Свойства обозревателя*.

В последней версии Internet Explorer появилось много новых функций, в том числе функция настройки вариантов создания cookie-файлов. Можно установить режим блокировки создания cookie-файлов. Следует различать два их типа: основные (firstparty) и сторонние (third-party). Основные cookie-файлы размещаются на компьютере тем сайтом, который посетил пользователь. Сторонние cookie-файлы размещаются на компьютере удаленными сайтами (например, рекламными).

Если нежелательно получение и, следовательно, хранение сторонних cookie-файлов, нужно сделать следующее:

1) Открыть новое окно Internet Explorer, выбрать в меню *Сервис* команду *Свойства обозревателя* и перейти на вкладку *Конфиденциальность*.
2) Оставить ползунок уровня конфиденциальности в положении *Умеренно высокий* и щелкнуть по кнопке *Дополнительно*. Откроется окно *Дополнительные параметры конфиденциальности*.
3) Установить флажок *Перекрыть автоматическую обработку файлов* «cookie» и установить следующие параметры приема cookie-файлов: основные

«cookie» - принимать, сторонние «cookie» – запрашивать, всегда разрешать сеансовые «cookie».

4) Два раза щелкнуть по кнопке *ОК* для возврата в окно *Свойства обозревателя*, а затем его закрытия.

При работе пользователя с безопасным веб-подключением, реализуемым с помощью протокола SSL (Security Sockets Layer - слой защищенных сокетов), например, при работе со своей учетной записью в виртуальном магазине или банке, происходит шифрование данных, пересылаемых с веб-сервера на клиентскую машину. После получения данных браузер клиентской машины с помощью специального ключа дешифрует информацию и отображает ее на компьютере. Расшифрованный файл остается в каталоге Temporary Internet Files. Следовательно, он доступен всем, кто имеет возможность локально зарегистрироваться на компьютере.

Проблема решается средствами Internet Explorer следующим образом:

1) Открыть новое окно Internet Explorer, выбрать в меню *Сервис* команду *Свойства обозревателя* и перейти на вкладку *Дополнительно*.
2) Найти в списке группу флажков *Безопасность*. Установить флажок *Не сохранять зашифрованные страницы на диске*.
3) Щелкнуть по кнопке *ОК* для сохранения и активизации сделанных изменений.

Функция автоматического заполнения URL-адресов, вводимых в адресной строке браузера, снижает уровень конфиденциальности, поэтому целесообразно очистить файл с историей вводившихся ранее адресов. Однако это не единственная ситуация, в которой срабатывает функция автоматического заполнения.

Система выдает список возможных вариантов и в том случае, когда заполняются поля ввода на веб-страницах. Эта особенность позволяет любому пользователю компьютера видеть, что искали другие пользователи на данном сайте, даже если журнал посещений сайтов в браузере был очищен. Следовательно, функция автоматического заполнения представляет угрозу конфиденциальности информации. Эту проблему можно решить следующим образом:

1) Открыть новое окно Internet Explorer, выбрать в меню *Сервис* команду *Свойства обозревателя* и перейти на вкладку *Содержание*.
2) Щелкнуть по кнопке *Автозаполнение*.
3) После открытия окна *Настройки автозаполнения* сбросить все флажки в группе *Использовать автозаполнение для*. Это позволит решить проблему, связанную с функцией автоматического заполнения.
4) В окне *Настройка автозаполнения* можно щелкнуть по двум кнопкам для удаления всех данных, хранящихся в журналах автоматического заполнения.
5) Щелкнуть по кнопке *ОК* для сохранения и активизации сделанных изменений.

Выше говорилось об удалении временных файлов Интернета. Удобно, если это делается автоматически при закрытии обозревателя. Для этого на вкладке *Дополнительно* окна *Свойства обозревателя* нужно установить флажок *Удалять все файлы из папки временных файлов Интернета* при закрытии обозревателя.

Интерфейс Windows. Проводник Windows сохраняет информацию о запускаемых пользователем приложениях и открываемых файлах. Это делается для удобства работы пользователя, т.к.ускоряет его работу, однако, отрицательно сказывается на уровне конфиденциальности, поскольку любой пользователь компьютера может увидеть, с какими программами чаще работает другой пользователь.

Если в целях сохранения конфиденциальности нужно очистить список часто запускаемых приложений, следует выполнить следующие шаги:

1) Щелкнуть правой кнопкой мыши по кнопке *Пуск* и выбрать в контекстном меню команду *Свойства*.
2) На вкладке *Меню* «*Пуск*» открывающегося окна щелкнуть по кнопке *Настроить*.
3) Щелкнуть по кнопке *Очистить список*.
4) Щелкнуть по кнопке *ОК* для закрытия окна *Настройка меню* «*Пуск*».
5) Еще раз щелкнуть по кнопке *ОК* для закрытия окна *Свойства панели задач* и меню «*Пуск*».

Система сохраняет информацию обо всех файлах, которые открывает пользователь. Это позволяет поддерживать список нескольких последних открывающихся файлов любого типа. Для сохранения в секрете перечня документов, с которыми работает пользователь, целесообразно периодически очищать список последних открывавшихся файлов. Сделать это можно следующим образом:

1) Щелкнуть правой кнопкой мыши по кнопке *Пуск* и выбрать в контекстном меню команду *Свойства*.
2) На вкладке *Меню* «*Пуск*» открывающегося окна щелкнуть по кнопке *Настроить*.
3) После открытия окна *Настройка меню* «*Пуск*» перейти на вкладку *Дополнительно*.
4) Щелкнуть по кнопке *Очистка списка.*
5) Щелкнуть по кнопке *ОК* для закрытия окна *Настройка меню* «*Пуск*».
6) Еще раз щелкнуть по кнопке *ОК* для закрытия окна *Свойства панели задач* и меню «*Пуск*».

Со временем жесткий диск может заполниться временными файлами, которые создают операционная система и некоторые приложения. Эти файлы могут быть использованы для анализа действий пользователя и, кроме того, занимают дисковую память. Поэтому следует периодически очищать диск от таких файлов. В системе имеется служебная программа *Очистка диска*. Для ее запуска следует выполнить команды *Пуск*®*Программы*®*Стандартные*® ® *Служебные* ® *Очистка диска*. После запуска программы откроется окно:

надо выбрать имя диска, на котором требуется удалить временные файлы, после чего нажать кнопку *ОК*. Через некоторое время открывается окно с перечнем файлов, которые можно удалить.

Существуют программы сторонних производителей, которые автоматически находят каталоги с временными файлами и очищают их. Популярна утилита TempCleaner, которую можно загрузить со многих веб-сайтов.

При посещении веб-сайтов, требующих аутентификации, или подключении к удаленным компьютерам пользователю часто предлагается сохранить пароль, чтобы при следующем доступе к сайту не приходилось вводить пароль заново. Данный режим удобен для пользователя, но создает дополнительную уязвимость в системе безопасности, поскольку любой другой пользователь, имеющий доступ к этому же компьютеру, сможет воспользоваться чужим именем и паролем, даже если он их не знает.

Удаление сохраненных паролей с компьютера позволит защитить свои учетные записи и повысить уровень их конфиденциальности. Предлагается следующий способ доступа к списку паролей:

1) В главном меню выбрать команду *Выполнить*.
2) В поле ввода открывшегося окна набрать строку rundll32.exe keymgr.dll.KRShowKeyMgr и щелкнуть по кнопке *ОК*.
3) Откроется окно *Сохранение имен пользователей и паролей* со списком всех учетных записей, сохраненных на компьютере.
4) Для удаления сохраненного пароля выбрать в списке нужную учетную запись и щелкнуть по кнопке *Удалить*.
5) Щелкнуть по кнопке *ОК* в диалоговом окне подтверждения, и учетная запись будет удалена из списка.
6) Повторить предыдущие шаги для всех учетных записей, которые нужно удалить.
7) Закончив удаление, щелкнуть по кнопке *Закрыть*.

На компьютерах с операционной системой Windows XP/2000/2003, использующих файловую систему NTFS, можно устанавливать разрешения на доступ к файлам и папкам. Это может быть очень мощным инструментом в обеспечении конфиденциальности информации.

Чтобы установить полный контроль над разрешениями на доступ, нужно сначала отключить режим общего доступа к файлам. Для этого следует открыть любую папку, в меню *Сервис* выбрать команду *Свойства папки*, перейти на вкладку *Вид* и сбросить флажок *Использовать простой общий доступ к файлам*. Далее можно перейти к настройке разрешений на доступ к требуемым папкам и файлам. Кроме того, для защиты данных в файловой системе NTFS можно их зашифровывать.

Задание для выполнения лабораторной работы:

Задание 1.

1 Настройте брандмауэр Windows XP. Определите список программ, которым разрешено обрабатывать данные, поступающие в компьютер из внешнего окружения. Не нужно ли сократить этот список?
2 Установите брандмауэр ZoneAlarm (предварительно отключив брандмауэр Windows XP, чтобы не допустить конфликтов). Определите, какие ваши приложения пытаются посылать данные в Интернет.

Задание 2.

1 Запустите оснастку *Службы*. Просмотрите список установленных и работающих служб. Все ли они необходимы для вашей повседневной работы. Удалите ненужные службы.
2 Загрузите с веб-сайта программу SpamKiller. Настройте программу (установите параметры фильтрации сообщений). Проверьте, установлен ли режим блокировки внешних ссылок в почтовой программе.

Задание 3.

1 Установите и обновите утилиты Ad-ware и Spybot S&D. Проверьте компьютер с помощью этих программ. Удалите обнаруженные spyware- и adware-программы. Проведите вакцинацию компьютера.
2 Проверьте параметры настройки браузера. Запретите загрузку элементов ActiveX.

Задание 4.

1 В целях конфиденциальности вашей информации проведите очистку четырех частей данных браузера: списка вводившихся адресов, журнала с историей посещения веб-сайтов, списка временных файлов Интернета и списка cokie-файлов.
2 Измените интерфейс Windows компьютера в целях повышения конфиденциальности вашей работы на компьютере:

- очистите список часто запускавшихся приложений;
- очистите список последних открывавшихся документов;
- удалите временные файлы с жесткого диска;
- удалите сохраненные пароли;
- назначьте необходимые разрешения к файлам и папкам;
- зашифруйте важную для вас информацию.

Контрольные вопросы

1 Какие разновидности атак Вы знаете?
2 Какие функции по защите компьютера выполняет брандмауэр?
3 В чем заключается основное функциональное различие между брандмауэром Windows XP и брандмауэром, различие между ZoneAlarm?
4 Как сделать компьютер невидимым в сети для других компьютеров?
5 Какие службы можно отключить с целью обеспечения безопасности компьютера? Как это сделать?
6 Что такое спам? Какие методы его распространения Вы знаете?

7 Какие способы борьбы со спамом Вы знаете?
8 Какие типы вредоносного программного обеспечения Вы знаете?
9 Какие применяются способы обнаружения и борьбы с вредоносным программным обеспечением?
10 Какая информация о действиях пользователя сохраняется в целях обеспечения комфортности его работы?
11 Какие действия следует предпринять, чтобы в целях конфиденциальности удалить с компьютера информацию о действиях пользователя?

Список литературы

1 Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
2 Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.
3 Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с.
4 Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. - 384 с.
5 Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга.. - М.: ЮНИТИ-ДАНА, 2013. - 239 с.
6 Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ, 2013. - 239 с.
7 Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография. / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ, 2015. - 239 с.

Содержание

Св.план 2017 г., поз. 72

Сауанова Клара Тагаевна

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ УПРАВЛЕНИЯ

Методические указания по выполнению лабораторных работ

для студентов специальности

5В070200 – Автоматизация и управление

Редактор Л.Т.Сластихина

Специалист по стандартизации Н.К.Молдабекова

Подписано в печать __.__.__
Тираж 70 экз.
Объем _2.4_уч.-изд.л.

Формат 60х84 1/16
Бумага типографская №1
Заказ____. Цена 1187_тг.

Копировально-множительное бюро

некоммерческого акционерного общества

«Алматинский университет энергетики и связи»

050013 Алматы, ул.Байтурсынова, 126