9. Горбенко І. Д., Долгов В. І., Гріненко Т. О. Інформаційна війна -- сутність, методи та засоби ведення // Матер. ювілейної наук. -техн. конф. «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». – Київ, 1998. – С. 11–15.
10. Гриняев С. Н. Информационная война: история, день сегодняшний и перспективы (http://www. agentura. ru).
11. Леваков А. Новые приоритеты в информационной безопасности США (http://www. agentura. ru).
12. Слипченко С. Информационное противоборство в бесконтактных войнах (http://kiev-security. org. ua).
13. Гриняев С. Н. Особенности информационной войны во время агрессии НАТО против Югославии (http://www. agentura. ru).
14. Ешихара Т. Китайская информационная война (http://abirus. ru).
15. http://www. crime-research. org. ua: Центр исследования проблем компьютерной преступности.
16. Интервью бывшего директора ФАПСИ А. Старовойтова (http://www. agentura. ru).
17. Красноступ Н., Кудин Д.. Шпионские программы и новейшие методы защиты от них // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Наук. -техн. збірник. Випуск 9. – Київ, 2004. – С. 67–75.
18. Барсуков В. С., Дворянкин С. В., Шеремет И. А. Методы и средства обеспечения безопасности в информационно-вычислительных сетях общего пользования// Технологии электронных коммуникаций. – Т. 20. – М.: 1992. – С. 65-96.
19. Климов В. Промышленный шпионаж как основа информационных войн (http://www. fakt. ru).

Поступила 3.03.2008г.

УДК 004.683

С.А. Печень

АНАЛИЗ РАБОТЫ СУЩЕСТВУЮЩИХ ТЕХНОЛОГИЙ ЗАЩИТЫ ИНФОРМАЦИИ КОРПОРАТИВНЫХ СЕТЕВЫХ РЕСУРСОВ

Наиболее распространенные средства защиты, согласно ежегодным отчетам CSI/FBI Security Survey, данные за 2007 год представлены в таблице 1[1]:

Таблица 1

Наиболее часто используемые технологии безопасности[2,3]

Место	Используемая технология	Процент использования данной технологии
1	Антивирусное ПО	98
2	Межсетевые экраны	97
3	Виртуальные частные сети	84
4	Антишпионское ПО	80
5	Системы обнаружения вторжений	69
6	Шифрование передаваемых данных	66
7	Управление обновлениями	63
8	Списки управления доступом	56

Продолжение таблицы1

9	Статические учетные записи/пароли	51
10	Шифрование данных в хранилищах информации	47
11	Системы предупреждения вторжений	47
12	Межсетевые экраны уровня приложений	45
13	Программное обеспечение управлением журналированием событий	44
14	Смарт карты/одноразовые пароли	35
15	Инфраструктура открытых ключей	32
16	Специализированные системы безопасности беспроводных сетей	28
17	Клиентское программное обеспечение конечного пользователя	27
18	Системы биометрической аутентификации	18
19	Другие	4

Стоит отметить, что основой исследования, один из результатов которого сведен в таблицу 1, является многовариантный опрос специалистов различных предприятий, различной формы собственности, различного направления деятельности и размера. Стоит отметить, что, к сожалению, подобных исследований на Украине пока не производится.

Рассмотрим функционирование первых двух технологий, на примере одного из отечественных предприятий.

Наиболее часто задействованная технология - использование комплексной системы антивирусной защиты, которая, как правило, включает в себя программные системы защиты серверов, рабочих станций и каналов приема/передачи электронной почты.

1. Рассмотрим статистику функционирования почтового шлюза за 2007 год.

1.1. Стоит отметить, что в данном случае, для защиты периметра использовались комплексное антивирусное и антиспамовское решение.

Согласно отчетам системы защиты почтового шлюза, всего за 2007 год поступило 590 230 тыс. сообщений. Из них зафиксировано и отказано в доставке около 500 тыс. сообщений с зафиксированным наличием вирусного кода (таблица №2). Примем во внимание, что в отличие от исследований предыдущих лет программное обеспечение противодействия вредоносному ПО разделено на различные категории - антивирусное и антишпионское. Хотя, в последнее время антивирусное и антишпионское ПО, как правило, разработчики интегрируют в одно решение, с целью достижения максимальной эффективности защиты информации клиента, следуя за разработчиками вредоносного кода, которые в свою очередь для достижения максимального значения количества зараженных ПК за минимальное время используют самые разнообразные технологии и их совокупности. Причем злоумышленники ставят основную цель - похищение конфиденциальной информации пользователя [4]. Таким образом, антивирусное и антишпионское программное обеспечение на практике стоит рассматривать комплексно, поскольку, если пропустить внутрь сети, например, шпионский модуль, он за собой подтянет, и модуль рассылки спама, и модуль своего распространения по вирусному принципу и другие модули [5].

Сообщений, расцененных как спам порядка 60% от общей суммы, или порядка 350 млн. в абсолютном исчислении.

Таблица 2

Статистика работы почтового шлюза, тыс. сообщений

Дата	Сообщений доставлено	Отказано в доставке, по причине					
		Наличие вирусного кода	Нахождение отправителя в списках распространи-телей спама	В имени присутствуют слова: dialup, dsl,pool,dhcp…	Нет соответствия имени ip адресу	Неизвестен получатель	прочие
31.01.2007	4 617	171	6 869	3 461	3 232	9 069	3 591
28.02.2007	4 095	49	6 825	1 815	3 956	9 633	4 125
31.03.2007	3 415	34	6 882	1 597	3 488	8 310	2 874
30.04.2007	3 524	33	9 910	2 013	3 142	8 814	3 445
31.05.2007	1 834	17	15 093	394	3 316	7 206	2 409
30.06.2007	1 810	22	25 818	534	4 318	5 321	3 301
31.07.2007	2 989	54	33 602	715	5 781	5 079	4 835
31.08.2007	2 937	19	50 836	1 037	10 040	3 906	2 217
30.09.2007	2 751	22	51 216	2 436	10 285	3 054	2 422
31.10.2007	1 824	13	45 522	1 073	5 515	658	1 669
30.11.2007	4 055	15	57 331	2 969	7 419	3 077	4 262
31.12.2007	5 856	51	38 414	7 666	7 766	2 759	5 699
Всего	**39 709**	**500**	**348 318**	**25 709**	**68 258**	**66 887**	**40 850**
% от общего количества почтовых сообщений	**6,73**	**0,08**	**59,01**	**4,36**	**11,56**	**11,33**	**6,92**

Стоит отметить, что «нормальная» корпоративная почта составила порядка 6,73% от общего количества рассылаемых почтовых сообщений, а в абсолютном выражении порядка 40 млн. сообщений в год. Данная цифра выглядит несколько завышено, однако стоит отметить что сюда, например, входят сообщения о подтверждении доставки абоненту, а также сообщения о прочтении адресатом направленной ему почты. Сюда также входят сообщения технического плана о состоянии функционирования различного рода технических средств, серверного и иного оборудования.

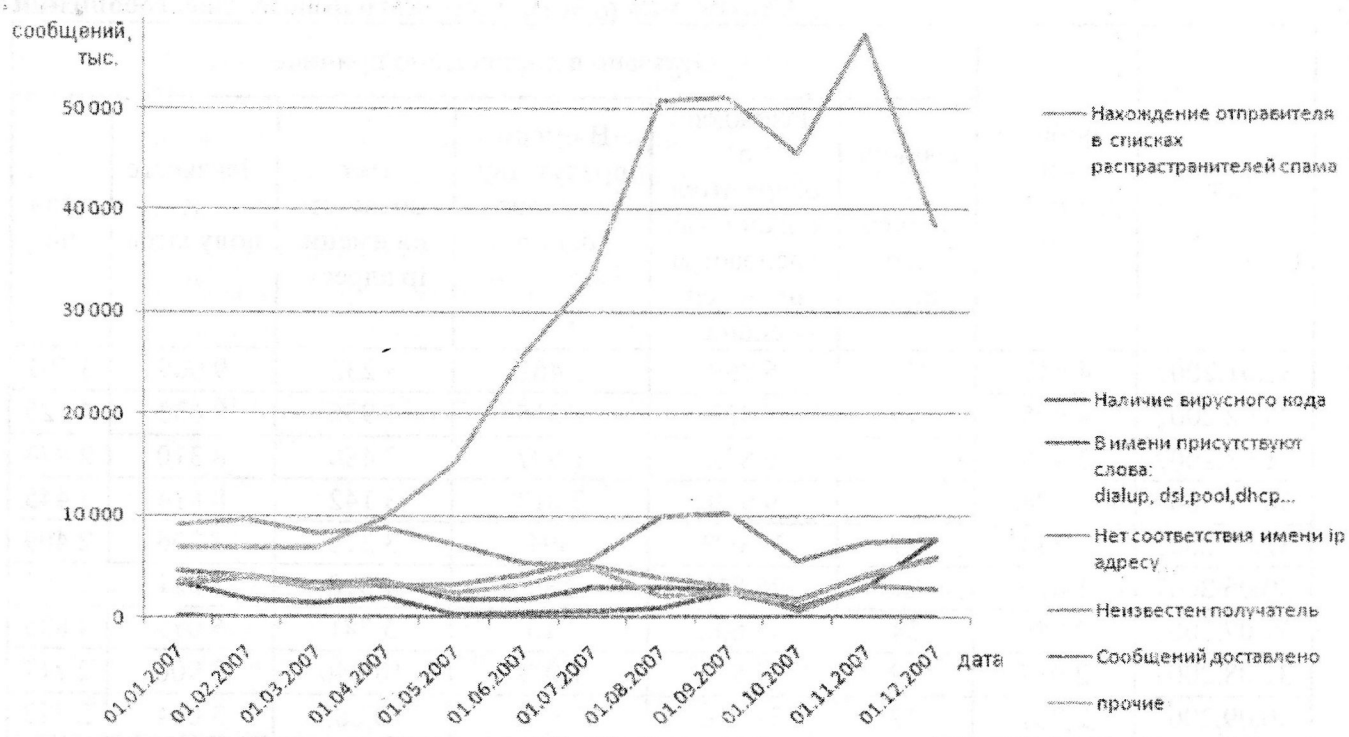

Рис. 1. Динамика почтовых сообщений за 2007год

Если рассмотреть динамику почтовых сообщений за 2007год, то на графике (рис.1) отчетливо наблюдается рост зафиксированного спама с адресов в черных списках (далее спама) продолжавшийся в течении II и III кварталов 2007года и стабилизировавшийся на уровне 50 млн сообщений в месяц в IV квартале. Резкого роста в других категорях не отмечено, следовательно можно сделать следующие заключения:

- количество спама с начала года выросло практически в 5 раз (с 10 млн до 50 млн сообщений в месяц);

- на фоне спада количества спама к концу 4 квартала отмечаем отсутствие роста и в других категориях, в связи с чем можно сделать предположение об эффективности технологии блокировки спама по «черным спискам», а также применяемых конкретных решений.

- в связи с отсутствием аномалий в других графах можно сделать заключение, что зафиксированный рост колическва спама соответствует реальному положению вещей.

Как факт стоит отметить, что количество вирусосодержащих сообщений составило незначительный процент от общего объема - порядка 0,08% от общего количества сообщений.

График зафиксированный на начало года под почти 10 млн. сообщений в месяц и к концу года стремящийся на спад - сообщения с несуществующим адресатом. Стоит отметить, что появление «нормальной» почты в таких объемах маловероятно, соответственно это:

- либо почта с технических средств, что тоже маловероятно в таких объемах, на протяжении длительного периода до обнаружения и локализации. Это возможно было бы лишь в разовых случаях, что выражалось бы пиковыми значениями;

-либо, что более вероятно, это спам.

В таком случае, в связи со спадом к концу года, количества электронных сообщений (электронной почты) на несуществующие корпоративные адреса, можно связать с появлением уточненных корпоративных адресов в базах данных спамеров.

График, который в августе-сентябре, практически не перешагнул границу в 10мн сообщений - сообщения с несоответствием имени отправителя его ip-адресу. Само по себе

получение почтового сообщения с неправильным обратным адресом - частный случай «отказа от авторства», являющийся отдельным видом нарушения защиты.

1.2. Рассмотрим функционирование антивирусной защиты внутренних узлов.

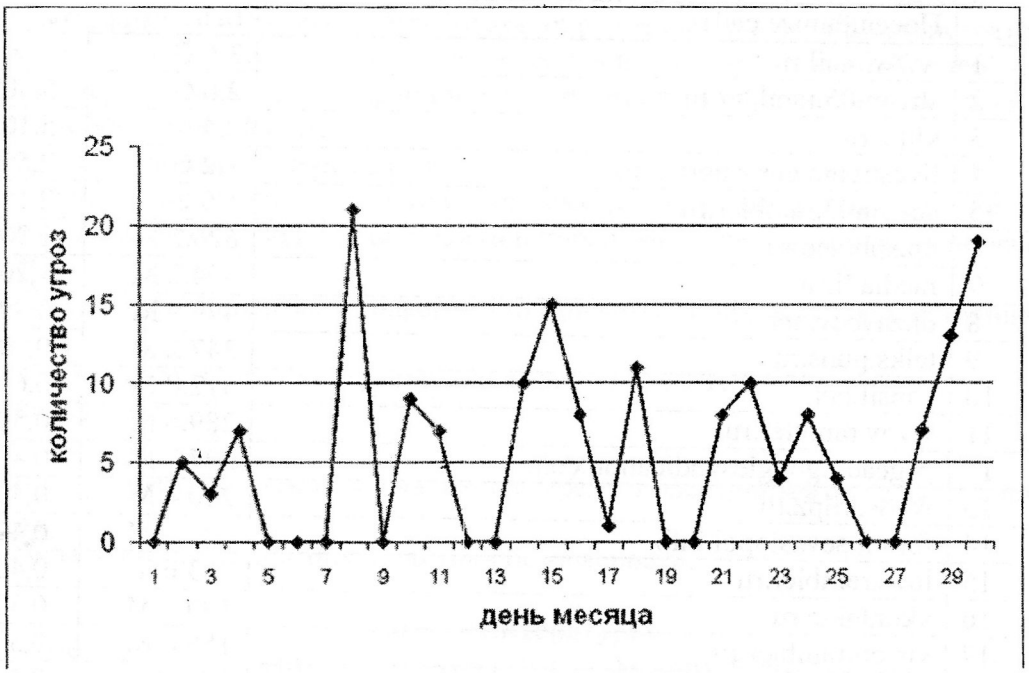

Рис. 2. График вирусной активности на внутренних узлах отдельно взятого сегмента сети порядка 500 АРМ за январь.

На данном графике хорошо видно, что спад вирусной активности приходится на выходные дни, когда машины попросту не включены.А вирусная активность не носит характера эпидемий.

В сопоставлении с общим количеством угроз поступающих в сеть , например по электронной почте (около 500 тыс. в год) пиковые значения около 20 единиц, к тому же, оперативно локализуемые иной, чем на почтовом шлюзе системой, выглядят несущественно.

2. Еще одним каналом угроз безопасности корпоративной сети передачи информации (далее КСПИ) предприятия, является подключение ее к сети Интернет. Для защиты периметра КСПИ используется межсетевой экран.

В процессе эксплуатации был зафиксирован инцидент выразившийся в аномальном повышении активности определенных хостов по портам. Было принято решение о мониторинге портов TCP 2041 и 2042.

Анализ причин появления повышенного исходящего трафика показал, что частые запросы к адресам, принадлежащим домену mail.ru, посылались программой Mail.ru Agent, обнаруженной на 8 АРМ КСПИ.

Mail.Ru Agent не требует прав администратора при установке, не является вредоносным ПО (и, соответственно, не обнаруживается антивирусами), поэтому предупредить появление данной программы (или аналогичной) в дальнейшем не представляется возможным.

По результатам расследования инцидента, порты на которые обращается Mail.Ru Agent, закрыты на межсетевом экране, а любая активность на этих портах заносится в протокол.

3. Доступ пользователей к ресурсам сети Интернет, как правило, проходит через корпоративный кэширующий прокси-сервер, что позволит:

- минимизировать трафик, и соответственно финансовые затраты предприятия,

-ограничить доступ корпоративных пользователей к нежелательным ресурсам.
Пример посещаемости сайтов:

Таблица 3

Пример статистики посещений 40 сайтов с наибольшим трафиком за один произвольно выбранный месяц в 2008 году на крупном предприятии (500 ПК)

№	Посещённые сайты	Байт	%
1	www.mail.ru	3.6 G	7,60%
2	stream05.rambler.ru	2.6 G	5,30%
3	klipz.ru	2.4 G	5,10%
4	livestream.eurosport.com	1.2 G	2,50%
5	stream03.rambler.ru	1.0 G	2,10%
6	up.spbland.ru	626.2 M	1,20%
7	media.li.ru	594.2 M	1,20%
8	dl.zaycev.net	479.9 M	0,90%
9	talks.guns.ru	347.2 M	0,70%
10	kapsil.net	312.0 M	0,60%
11	www.rambler.ru	289.6 M	0,50%
12	pagead2.googlesyndication.com	227.7 M	0,40%
13	www.klipz.ru	220.4 M	0,40%
14	forum.sevastopol.info	207.4 M	0,40%
15	love.rambler.ru	203.6 M	0,40%
16	vkontakte.ru	190.1 M	0,30%
17	vision.rambler.ru	185.6 M	0,30%
18	fpdownload2.macromedia.com	181.1 M	0,30%
19	img.readme.ru	180.4 M	0,30%
20	de.fishki.net	177.3 M	0,30%
21	www.download.windowsupdate.com	155.1 M	0,30%
22	mail.rambler.ru	154.2 M	0,30%
23	i.i.ua	151.5 M	0,30%
24	smex-p.activeupdate.trendmicro.com	150.3 M	0,30%
25	uletno.info	149.7 M	0,30%
26	an.yandex.ru	146.0 M	0,30%
27	gak.com.ua	144.1 M	0,20%
28	www.gismeteo.ua	140.9 M	0,20%
29	www.foxconnchannel.com	132.3 M	0,20%
30	www.marketgid.com	132.2 M	0,20%
31	Support.xx.ukrtelecom.ua	126.0 M	0,20%
32	195.161.xxx.xxx	123.0 M	0,20%
33	www.yandex.ru	121.4 M	0,20%
34	pimg.dt00.net	121.2 M	0,20%
35	travel.org.ua	118.2 M	0,20%
36	www.segodnya.ua	117.2 M	0,20%
37	download.zachot.ru	115.9 M	0,20%
38	www.reedlan.com	115.1 M	0,20%
39	olegmityaev.ru	115.0 M	0,20%
40	www.ray-s.de	114.2 M	0,20%

Стоит отметить, что наиболее посещаемые сайты сложно причислить к перечню необходимых по служебным делам, например vkontakte.ru (социальная сеть общения

одноклассников) или klipz.ru (клипы). Соответственно политика безопасности на предприятии, и конкретная ее реализация на прокси-сервере требует корректировки.

Наличие сайта www.download.windowsupdate.com (обновления операционных систем разработки Microsoft corp.) в перечне целевых сайтов, указывает на необходимость создания локального корпоративного сайта обновлений программного обеспечения фирмы Microsoft для минимизации трафика. Либо может потребовать обращения внимания администратора сети на сетевые ПК, неподключенные к локальному серверу обновлений, так как ПК с необновляемой с необходимой периодичностью операционной системой могут оказаться узким местом безопасности корпоративной сети.

Причины возникновения инцидентов:

- несвоевременные обновления антивирусных баз данных, либо появление новых видов программного обеспечения, ведущего несанкционированную деятельность, и не являющегося вирусным ПО;
- использование внешних носителей информации (дискеты, flash-диски), как источников заражения;
- подключение к сети Интернет внутренних пользователей КСПИ;
- человеческий фактор.

Заключение:

Используемые технологии, являются в настоящее время эффективным средством защиты информации.

Методы защиты: совершенствование политики безопасности.

Список литературы

1.2007 CSI/FBI Computer Crime and Security Survey, http://www.gocsi.com/forms/csi_survey.jhtml

2. Хорошко В.А., Чекатков А. А. Методы и средства защиты информации/Под. ред. Ю.С. Ковтанюка. - К.:Юниор, 2003.- 504 с.
3. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты.-К.:ООО «ДС», 2001.-688 с.
4. В.А. Хорошко проф., д.т.н., С.А. Печень. Прикладные аспекты современных сетевых нефизических парольных атак и парольной защиты// Захист інформації, Спецвипуск, 2007 – с.88-94

Поступила 3. 03.2008г.

УДК.681.3.06(075)

С.Р.Коженевский, С.А.Чеховский

СПОСОБ ПОСТРОЕНИЯ ЗАЩИЩЕННОЙ ЛОКАЛЬНОЙ СЕТИ ДЛЯ ОБРАБОТКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, ОСНОВАННЫЙ НА МОДУЛЬНОМ ПРИНЦИПЕ

Построение локальной вычислительной сети с защитой информации от утечек по каналам ПЭМИН представляет собой сложную техническую задачу. Для решения этой задачи, в отличие от задачи защиты одиночного ПК, необходимо обеспечить экранирование всех элементов локальной сети - серверов и рабочих станций, активного и пассивного сетевого оборудования, распределенных в пространстве на значительные расстояния. Кабельная система локальной сети, как правило, выполненная на основе витой пары (экранированной либо неэкранированной), выполняет роль антенной системы для паразитных излучений элементов ПК и активного сетевого оборудования, эффективность и диаграмма