Продолжение таблицы 2

RIJNDAL	128	256
3-ключевой 3-DES	168	336
RIJNDAL	192	384
RIJNDAL	256	512

Выводы

Использование протоколов установления и выработки ключей в группах точек эллиптической кривой позволяет согласованно выработать ключи и обеспечить функцию причастности. Использование преобразований в группах точек ЭК по сравнению с преобразованиями в кольцах и полях [3] позволяет в 4 – 6 и более раз сократить длины открытых ключей и общесистемных параметров, или при тех же параметрах существенно повысить стойкость.

Используемые на практике состоятельные протоколы, реализуемые за счет преобразований в кольцах и полях, являются состоятельными и при использовании в группах точек эллиптических кривых.

Следует ожидать, что в ближайшие годы при реализации состоятельных протоколов будут использоваться алгоритмы направленного шифрования, цифровой подписи и выработки ключей, построенные на основе преобразований в группах точек эллиптической кривой.

Литература: 1. X9.42 Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Algorithm Keys Using Diffie-Hellman, 1996. Working Draft. 2. X9.63 Public Key Cryptograph For The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography. 1999. 207 с. 3. Криптографические преобразования в группах точек эллиптических кривых методом Полларда / И. Д. Горбенко, С. И. Збитнев, А. А. Поляков // Радиотехника: Всеукр. межвед. науч.-тех. сб. 2001. Вып. 119. с. 43 –50. 3. http://crypto.nessie.org

УДК 681.3

СРАВНИТЕЛЬНЫЙ ОБЗОР АНТИВИРУСНЫХ ПРОДУКТОВ ДЛЯ РАБОЧИХ СТАНЦИЙ НА БАЗЕ ОС WINDOWS

Олег Сыч
ООО "Украинский Антивирусный Центр"

Аннотация: **Дан анализ технических характеристик ведущих антивирусных продуктов, обеспечивающих возможность комплексной антивирусной защиты локальной сети.**
Summary: **The analysis of characteristics of conducting anti-virus products ensuring an opportunity of complex anti-virus protection of a local network.**
Ключевые слова: **Информационная безопасность, антивирусная безопасность.**

На сегодняшний день рынок антивирусных продуктов представлен наиболее крупными и известными продуктами: Norton Antivirus [1], McAfee, KAV [2] (ранее AVP) и DrWeb. Кроме того, стоит отметить также продукт отечественной разработки UNA. Каждый из продуктов обладает своими достоинствами и недостатками. Как правило, для комплексной защиты локальной сети и серверов рекомендуется применять несколько различных антивирусных продуктов, но при этом на одном компьютере должно стоять не более одного антивируса.

При выборе антивирусных продуктов, как правило, руководствуются следующими параметрами:

1. Вирусная база продукта.
2. Известность продукта и компании разработчика.
3. Стабильность работы и удобство пользования.
4. Стоимость продукта.
5. Качество технической поддержки.
6. Страна происхождения.

С точки зрения национальной безопасности важное значение имеет происхождение антивирусного продукта, особенно в сетях, где информация содержит государственную, банковскую или коммерческую тайну, в частности в государственных органах, а также после ряда громких скандалов, вызванных

выявлением фактов негласной передачи информации с компьютеров пользователей программными продуктами некоторых зарубежных производителей.

Проведём анализ предлагаемых на рынке продуктов. Для этого возьмём перечисленные выше продукты. В табл. 1 приведены данные о продукте, представленные компанией-разработчиком.

Таблица 1 – Информация о тестируемых продуктах

	Norton Antivirus	McAfee VirusScan	KAV Pers. PRO	***DrWeb***	UNA PRO
Версия продукта	Corp. Ed. V7.6	V5.01	V4.0	V4.27	V1.50
Разработчик	Symantec	Network Associates	Kasersky Lab.	Диалог наука	Украинский Антивирусный Центр
Web Сайт в Internet	Symantec.com	www.mcafee.com	kaspersky.ru	www.drweb.ru	unasoft.com.ua
Заявленная вирусная база	60877	>60000	53655	29426	40102

Несмотря на огромные разрывы в заявленных вирусных базах (от 29000 до 60000 вирусов) международные антивирусные тесты показывают, что все представленные продукты обнаруживают приблизительно одинаковое количество вирусов (отличие в обнаруживаемых вирусных базах не превышает 15%). Причиной такой разницы в заявленных вирусных базах является различная система подсчёта типов вирусов, а также завышение технических параметров в реальных целях. Проверить точную цифру не представляется возможным в связи с тем, что каждая вирусная коллекция уникальна.

Для сравнения вирусных баз проведём анализ динамики роста баз в течение последних двух лет. На рис. 1 представлены графики роста антивирусных баз, а в табл. 2 – технические параметры анализируемых антивирусных продуктов.

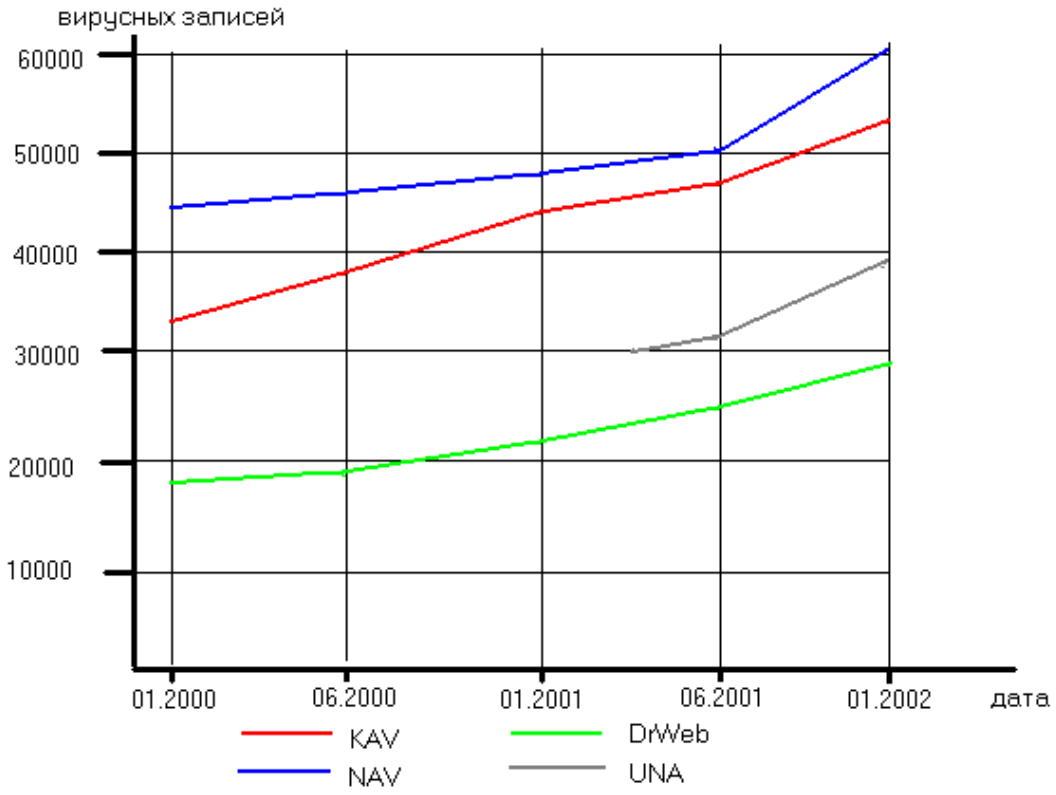

Рисунок 1 – Динамика роста антивирусных баз

Таблица 2 – Технические параметры анализируемых антивирусных продуктов

	NAV	McAfee	KAV	DrWeb	UNA
Планировщик заданий	+	+	+	+	+
Script-checker	+	–	+	–	+
Сканирование архивов	+	+	+	+	+
Сканирование почтовых баз	+	+	+	+	+
Сетевые решения	+	+	+	–	+

Для проверки качества и скорости тестирования различными антивирусами проводим тестирование всех вышеперечисленных продуктов на антивирусной базе в 42000 вирусов. Поскольку вирусы находятся не в дикой среде (на инфицированных компьютерах), а в коллекции (то есть присутствуют только файлы с телами вирусов), целью данного тестирования является проверка качества детектирования вирусов, но не их лечения.

При тестировании все антивирусные продукты были установлены на максимальный уровень тестирования (эвристические анализаторы включены на максимум). При этом срабатывание на вирусе эвристического анализатора также считалось детектированием вируса. В таблице 3 приводится количество пропущенных вирусов по типам (в скобочках проценты обнаруженных вирусов).

Таблица 3 – Число пропущенных вирусов по типам

Типы вирусов	Макро-вирусы (из 2700)	Обычные вирусы (из 25074)	Script-вирусы (из 810)	Троянские программы (из 3583)	Всего (из 32167)
NAV	63 (97.66 %)	2431 (90.30 %)	75 (90.74%)	1009 (71.84 %)	3578 (88.87 %)
McAfee	80 (97.03 %)	2854 (88.61 %)	13 (98.39 %)	872 (75.66 %)	3819 (88.12 %)
KAV	19 (99.29 %)	79 (99.68 %)	0 (100.0 %)	36 (98.99 %)	**134 (99.58 %)**
DrWeb	58 (97.85 %)	280 (98.88 %)	124 (84.69 %)	118 (96.70 %)	**580 (98.19 %)**
UNA	261 (90.33 %)	192 (99.23 %)	24 (97.03 %)	0 (100.0 %)	**477 (98.51 %)**

При тестировании наихудшие результаты показали продукты McAfee и NAV. Три остальных антивирусных продукта показали близкие к 100% результаты.

Следует отметить, что 100%-ого результата удалось достичь комбинированием антивирусных продуктов KAV и UNA, а при комбинировании продуктов DrWeb и UNA результат был близок к 100%.

При тестировании у каждого из продуктов был выявлен ряд недостатков:

1. Norton Antivirus:
   – низкая скорость тестирования (наиболее низкая из всех тестируемых продуктов);
   – большие объёмы антивирусных обновлений, получаемых через Internet;
   – отсутствие собственного планировщика заданий (используется планировщик заданий Windows);
2. McAfee VirusScan:
   – слабый уровень обнаружения вирусов;
3. Kaspersky AntiVirus:
   – высокое потребление ресурсов;
   – конфликты резидентного монитора с другим ПО;
4. DrWeb
   – низкая скорость работы;
   – нет сетевого решения;
   – отсутствие планировщика заданий;
5. Ukrainian National Antivirus (UNA):
   – резидентный монитор проверяет файлы только при запуске;

Кроме того, разработчики NAV (Symantec) и McAfee VirusScan (Network Associates) расположены на территории США, что затрудняет контакт непосредственно с разработчиками продуктов.

Комплексная защита организационной структуры подразумевает защиту следующих составляющих:

– рабочих станций локальной сети;
– сервера локальной сети;
– рабочих станций, не входящие в состав локальной сети;
– сервера доступа к глобальной сети Интернет.

При этом наибольшее внимание следует уделять точкам входа и обмена информацией.

Точки входа информации в локальной сети предприятия (рис. 2):

– Web сайты Internet;
– электронная почта;
– сменные накопители (Floppy, CD-ROM, ZIP-drive и т. п.);
– открытые для общего доступа папки соседних ПК.

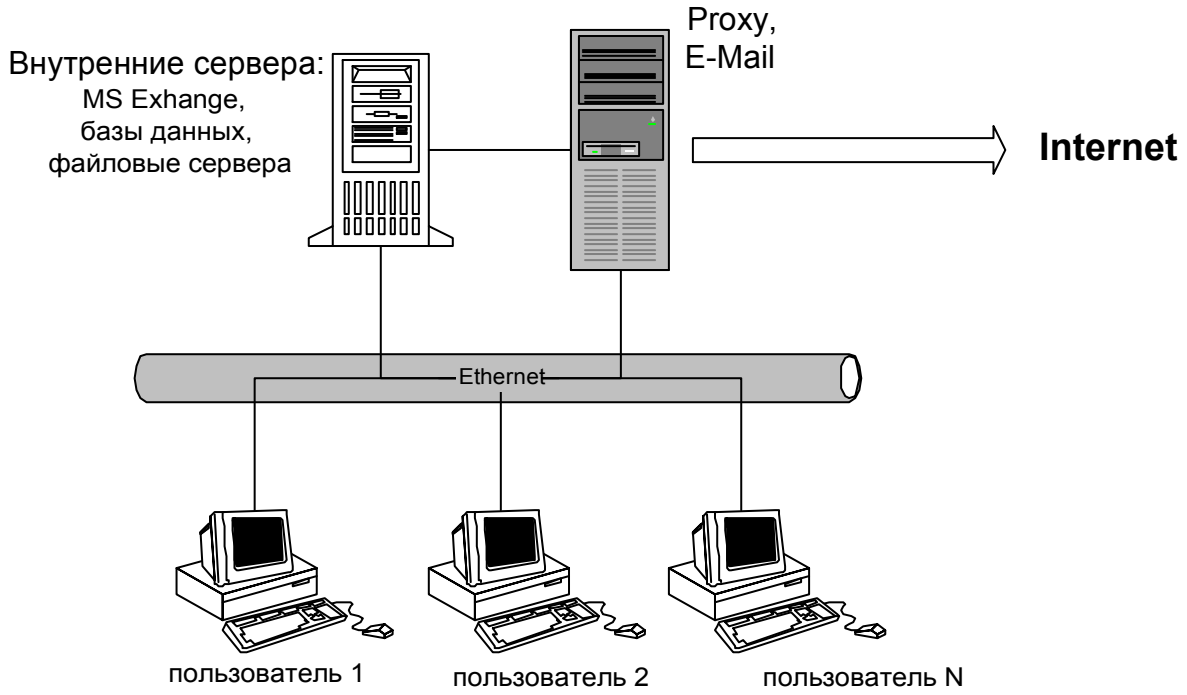

Рисунок 2 – Типовая организация локальной сети

Учитывая, что защищаемые ПК используются для активной работы персоналом, имеет смысл уменьшить нагрузку рабочих станций антивирусными пакетами.

Как правило, локальные сети крупных предприятий разнесены территориально на большие расстояния, что затрудняет контроль и управление централизованной антивирусной защиты, поэтому нельзя обойтись без корпоративных сетевых решений.

Корпоративные решения подразумевают, что на один из серверов (либо выделенный сервер) устанавливается серверная часть сетевой версии антивируса, на рабочие станции устанавливаются клиентские части. При этом на сервер ложатся задачи:

– получения антивирусных обновлений с Web сайтов разработчиков;
– централизованное управление клиентскими модулями;
– получение статистической информации в масштабах локальной сети.

Полнота реализации перечисленных функций в продуктах NAV, UNA, AVP представлена в табл. 4 (в порядке убывания возможностей сетевой версии).

Таблица 4 – Возможности сетевых версий продуктов.

Наименование продукта	Комментарии
NAV	Максимальные возможности централизованного управления, удалённая установка, удобство использования.
UNA	Наличие выделенного сервера, к которому подключаются клиентские модули. Удобство использования, минимальная загрузка системы.
AVP	Построение сетевой защиты на основе встроенного Центра Управления.

На сервера общего доступа и сервера доступа к глобальной сети Internet устанавливаются серверные решения антивирусной защиты. При этом необходимо рассматривать не только платформу, на которой установлен сервер, но также и серверы, которые он обслуживает.

Литература: 1. Norton AntiVirus Corporate Edition. Руководство по применению. 2. Kaspersky AntiVirus – руководство пользователя.

УДК 681.3.06

ОПРЕДЕЛЕНИЕ МНОЖЕСТВА МЕХАНИЗМОВ ЗАЩИТЫ, ОБЕСПЕЧИВАЮЩИХ ОПТИМАЛЬНЫЙ УРОВЕНЬ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

Алексей Новиков, Андрей Тимошенко*
Физико-технический институт НТУУ «КПИ»
**ООО «Институт компьютерных технологий»*

Аннотация: **Рассмотрены вопросы разработки аглоритма решения задачи определения множества механизмов защиты информации, обеспечивающих оптимальный уровень защищенности информации, обрабатываемой в компьютерной системе с открытой архитектурой.**
Summary: **The problems of development of the algorithm for determination a security mechanisms set that ensures an optimum level of an information security in the computer system with open architecture are considered.**
Ключевые слова: **Механизм защиты, стек протоколов, угроза информации.**

I Постановка задачи

Построение системы защиты информации (СЗИ), обрабатываемой в компьютерной системе (КС), предполагает, согласно [1], проведение анализа потенциальных угроз информации, оценки рисков, связанных с их реализацией (как функции вероятности реализации данных угроз и величины возможного ущерба). С учетом результатов проведенного анализа, должен быть проведен выбор для включения в СЗИ таких механизмов защиты, использование которых обеспечит максимальную защищенность обрабатываемой информации. При этом стоимость реализации средств защиты должна быть адекватна величине возможного ущерба. В [2] в качестве характеристики защищенности обрабатываемой в КС информации предложено использовать вероятность сохранения защищенности как функцию множества реализованных в СЗИ КС механизмов защиты $P(M)$. Там же получено следующее ее выражение для КС с открытой архитектурой и многоуровневым стеком протоколов [3]:

$$P(M)=\prod_{i=1}^{L}\left(\prod_{j=1}^{N}(1-E_{ij})+\sum_{j=1}^{N}\left[E_{ij}\prod_{k=1}^{j-1}(1-E_{ik})\cdot\left(\sum_{k=1}^{j}M_{ik}\cdot\prod_{l=k+1}^{j}(1-M_{il})\right)\right]\right) \qquad (1)$$

где L – количество потенциальных угроз информации, обрабатываемой в КС; N – количество уровней стека протоколов КС; M_{ij} – целочисленная переменная, значение которой определяет факт наличия/отсутствия механизма защиты от i-й угрозы на протоколе j-го уровня, $M_{ij}\in\{0,1\}$; E_{ij} – показатель эффективности реализации i-й угрозы на протоколе j-го уровня, характеризующий степень риска, связанного с реализацией данной угрозы, как функцию вероятности реализации угрозы и величины возможных потерь, $E_{ij}\in[0,1]$.

Адекватность стоимости реализации средств защиты величине потенциального ущерба предполагает наличие ограничения на максимальное значение затрат на реализацию СЗИ (стоимость реализуемых в СЗИ механизмов защиты). С учетом (1), данное ограничение для КС с открытой архитектурой можно сформулировать следующим образом:

$$C(M)=\sum_{i=1}^{L}\left(\sum_{j=1}^{N}M_{ij}\cdot C_{ij}\right)\le C_o \qquad (2)$$

где $C(M)$ – стоимость реализации множества механизмов защиты $M=\{M_{ij}\}$, $i\in\{1,...,L\}$, $j\in\{1,...,N\}$; C_{ij} – стоимость реализации механизма защиты от i-й угрозы на протоколе j-го уровня; C_o – максимальное значение затрат на реализацию СЗИ.