V Висновки

У роботі формалізовано модель оцінки ефективності функціонування алгоритмів шифрування інформації на ЕК. Дана модель не претендує на повноту, але розглядається як базова, є відкритою і може бути легко доповнена та деталізована в подальшому. Дана модель може бути використана для порівняльного аналізу та квазі-оптимального вибору алгоритму шифрування інформації на ЕК для практичної реалізації засобів захисту інформації. Особливістю вказаної моделі є те, що поряд із традиційними підходами вона дозволяє також враховувати стійкість алгоритму до сучасних атак.

*Література.**1**. Система показателей оценки эффективности функционирования схем поточного шифрования / А. В.Потий, Ю. А.Избенко // Радіотехніка:Всеукр. міжвід. наук.-техн. зб. 2003. вип.. 134. с. 49-61. **2**. К. Шеннон "Теорія зв`язку в секретних системах", 1949 р. **3**. Thomas Wollinger and Christof Paar. How Secure Are FPGAs in Cryptographic Applications. In 13th International Conference on Field Programmable Logic and Applications - FPL 2003, Lisbon, Portugal, September 1-3, 2003. **4**. А. Л. Чмора. Современная прикладная криптография. 2-е изд., стер. – М.:Гелиос АРВ, 2002. – 256 с.: ил. **5**. Молдовян А. А., Молдовян В. А., и др. Криптография. – Серия "Учебники для вузов. Специальная литература". – Спб.: Издательство "Лань", 2000. – 224 с., ил. **6**. Alexander Muir. Techniques of Side Channel Cryptanalysis. Thesis for the degree of Master of Mathematics in Combinatorics and Optimization, Waterloo, Ontario, Canada, 2001, p.92. **7**. Okeya, K., Sakurai, K., How to Implement Scalar Multiplication Algorithm on Elliptic Curves for Resisting against Power Attacks, Proceedings of the 2000 Engineering Sciences Society Conference of IEICE, A-7-13, (2000). **8**. Okeya K., Sakurai K., Power Analysis Breaks Elliptic Curve Cryptosystems even Secure against the Timing Attack, Progress in Cryptology – INDOCRYPT 2000, LNCS1977, (2000), 178-190. **9**. Smar , N .P., The Discrete Logarithm Problem on Elliptic Curves of Trace One, Journal of Cryptology, Vol.12, No.2, (1999), 141-151. **10**. М. Карпінський, І. Васильцов, І. Якименко, Я. Кінах, "Метод генерування параметрів еліптичних кривих", Правове, нормативне, та метрологічне забезпечення системи захисту інформації в Україні, Київ, випуск 6, с. 74, 2003. **11.** М. Карпінський, І. Васильцов, І. Якименко, А. Гончарик. Elliptic curve Parameters Generetion // Proceedings of the Integrational Conference TCSET'2004 "Modern problems of radio engineering, Telecomunications and computer science", february 24-28, 2004, p. 294-295*

УДК 681.31

ПРИНЦИПЫ ПОСТРОЕНИЯ КОМПЛЕКСНОЙ СИСТЕМЫ АНТИВИРУСНОЙ ЗАЩИТЫ

Сергей Емельянов, Игорь Яковлев
Одесская национальная юридическая академия

Аннотация: **Рассмотрены общие принципы построения комплексной системы антивирусной защиты (КСАЗ). Проанализированы основные составляющие КСАЗ, показаны проблемные аспекты их практической реализации.**
Summary: **In the article represents the basic principles of construction of complex system of anti-virus protection (CSAP). Basic components CSAP are analyzed, problem aspects of their practical realization are shown.**
Ключевые слова: **Компьютерные вирусы, комплексная система антивирусной защиты, правовые, организационные, программно-технические методы антивирусной защиты.**

I Введение

В настоящее время одной из реальных угроз конфиденциальности, целостности и доступности информации в компьютерных системах и сетях (КСС) являются компьютерные вирусы (КВ). Под КВ понимаются автономно функционирующие программы (программные коды), способные к самовключению в тела других программ и последующему самовоспроизведению и самораспространению в КСС [1 – 3].

Первые КВ появились в конце 80 годов. С этого времени их количество растет по экспоненциальному закону, достигая сегодня нескольких десятков тысяч видов.

Несмотря на достигнутые успехи в новом научном направлении – компьютерной вирусологии, новостийные WEB–сайты пестрят сообщениями о новых "успешных" и отраженных вирусных атаках и угрозах [4]. Несомненное лидерство среди КВ занимают сегодня почтовые сетевые черви, имеющие

программные механизмы самораспространения по электронным адресам, найденным в инфицированной КСС.

Хорошо известно, что современная комплексная система защиты информации должна основываться на сочетании различных методов, средств и механизмов защиты. Представляется актуальной задача рассмотрения данного интегрального подхода к построению КСАЗ с целью выявления "узких" мест и брешей в антивирусной защите, наличие которых обуславливает вирусную активность и постоянно растущие материальные потери владельцев и пользователей КСС.

II Основная часть

Главной задачей КСАЗ является профилактика и предупреждение пользователей КСС о вирусной атаке на ее ранних стадиях, а также блокировка потенциально опасных (вредоносных) воздействий на элементы КСС (информацию, носители, программно-математическое и аппаратное обеспечение и т. д.). Решение данной задачи возможно только на основе комплексирования различных методов, средств и механизмов защиты, главными из которых являются правовые, организационные и технические (рис. 1).

Правовые методы основаны на нормотворческой, исполнительной и правоприменительной деятельности, вводящей и поддерживающей административную и уголовную ответственность за умышленное создание и распространение КВ с целью нанесения ущерба. Например, диспозиция ст. 361 нового УК Украины [5] рассматривает в качестве одной из объективных сторон преступления распространение компьютерного вируса путем применения программных и технических средств, предназначенных для незаконного проникновения в КСС. Однако привлечение к ответственности за такое правонарушение законодатель увязывает с наступлением определенных последствий – искажение или уничтожение компьютерной информации либо носителей такой информации. Следует обратить внимание, что такая трактовка существенно снижает пределы ответственности за операции с вредоносными программами. В частности, определено наказание лишь за распространение КВ и оставлены без внимания другие общественно опасные деяния – создание и использование КВ, в отличие, например, от ст. 273 УК Российской Федерации.

Основные проблемные аспекты в применении правовых методов сегодня обусловлены следующими факторами:

-неоднозначность трактовки квалифицирующих признаков данного вида компьютерных преступлений;

-трудности в физическом обнаружении (задержании) злоумышленника;

-трудности в доказательстве авторства и умышленности в его действиях;

-отсутствие единых методик по оценке нанесенного ущерба.

Указанные факторы обуславливают бедность юридической практики применения правовых методов антивирусной защиты информации в Украине.

Организационные методы антивирусной защиты основаны на строгом соблюдении определенных технологических операций с носителями и источниками информации. Их направленность, полнота и жесткость во многом зависят от назначения и характера эксплуатируемой КСС. Например, в КСС на основе локальных рабочих станций (ЛРС) возможны три способа проникновения вирусов [2, 3]:

-поступление вместе с программным обеспечением, предназначенным для последующего использования в работе;

-занесение пользователями с программами, не относящимися к эксплуатируемой КСС;

-преднамеренное создание пользователями.

Вероятность проникновения вирусов первым путем можно значительно снизить, если разработать и поддерживать правильные процедуры приобретения, установки программ и контроля за внесением в них изменений. Процедура приемки должна быть достаточно продолжительной и всесторонней, в нее должны быть включены специальные операции по провоцированию известных вирусов. Так, например, после известной пандемии в Украине в конце 1994 г. нового полиморфного вируса OneHalf единый операционный день в большинстве банков страны теперь начинается, в том числе, с обязательного контроля состояния антивирусной защищенности своих КСС [6, 7].

Вероятность проникновения вирусов вторым путем можно уменьшить введением запрета на приобретение и запуск программ без специальной процедуры проверки. Возможен также частичный запрет на использование посторонних программ на определенных аппаратных средствах КСС.

Вероятность умышленного внедрения вируса в КСС внутренним персоналом можно существенно уменьшить, если с достаточным вниманием контролировать деятельность вычислительных центров и отдельных пользователей.

Очевидно, однако, что применение подобных методов защиты к локальным (глобальным) КСС объективно затруднено вследствие их распределенной архитектуры.

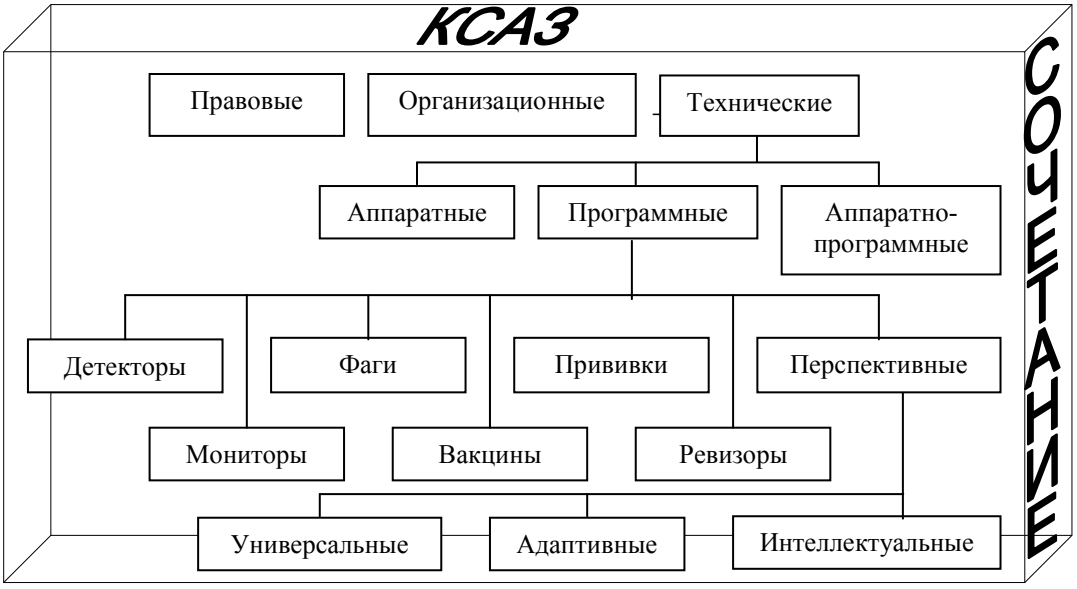

Рисунок 1 – Составляющие КСАЗ

Наиболее существенный вклад в решение задач антивирусной защиты сегодня вносят **технические методы,** основу которых составляют аппаратные, программные и программно-аппаратные методы и средства.

Самый простой способ аппаратной защиты – отключение от КСС всех физических каналов (устройств), через которые в нее может проникнуть вирус. Если это ЛРС, не подключенная к локальной сети, и на ней не установлен модем, то достаточно отключить накопители на ГМД. При этом основной канал возможной атаки вирусов будет заблокирован. Однако такое отключение не всегда возможно. В большинстве случаев пользователю необходим доступ к дисководам или модемам. Кроме того, зараженные программы могут проникать в КСС через локальную сеть (сетевые вирусы), а также через компакт-диски (CD-ROM вирусы), отключение которых значительно уменьшает возможности КСС. Разрабатываются и внедряются и более сложные способы защиты, основанные на аппаратной поддержке операционной системы (ОС) и контролирующих ее средств, реализуемые на специальных дополнительных платах. К ним относят:

запрет или регистрация попыток записи в файлы ОС и в области памяти, занятой системной информацией;

установление приоритета в обработке программ, составляющих ОС, и антивирусных средств перед программами пользователей;

разделение областей памяти, в которой работают программы, невозможность записи в другую область памяти;

выделение некоторых функций и возможностей ЭВМ, которые могут быть реализованы только программами ОС.

По существу, данные аппаратные средства позволяют контролировать все обращения к главной загрузочной записи жестких дисков, а также к загрузочным секторам дисков и дискет. В случае, если какая-то программа попытается изменить содержание загрузочных секторов (BIOS-вирусы, boot-вирусы), срабатывает защита и пользователь получает соответствующее предупреждение. Однако стоимость таких дополнительных плат достаточно высока.

Наиболее распространенными сегодня средствами нейтрализации вирусов являются **программные средства** антивирусной защиты. В настоящее время имеется большое число антивирусных программных средств как отечественного, так и зарубежного производства. Все антивирусные программы, исходя из реализованного в них подхода к выявлению и нейтрализации вирусов, принято делить на классы, показанные на рис. 1.

Детекторы являются наиболее старым классом средств программной защиты от вирусов. Их основное назначение – обнаружение КВ посредством последовательного просмотра всех файлов и поиска сигнатур – устойчивой последовательности байтов, имеющихся в телах известных вирусов.

Фаги выполняют функции, свойственные детекторам, но, кроме того, “излечивают” инфицированные программы посредством “выкусывания“ вирусов из их тел. При написании указанных программ необходимо

учитывать ряд особенностей:

-сигнатура должна обеспечивать надежное распознавание КВ в случае его модификации (например, изменение текстовых сообщений, выдаваемых вирусом);

-сигнатура должна быть достаточно длинной, чтобы исключить ложное срабатывание детектора.

Следует отметить, что эти факторы в некоторой мере противоречивы. Поэтому выбор сигнатуры является прерогативой разработчика, а не строго формализованной процедурой.

Преимущество программ-детекторов и фагов состоит в возможности однозначного определения наличия в КСС одного из нескольких фиксированных типов КВ, и, в некоторых случаях, оперативного излечения инфицированных программ. Кроме того, в силу общности алгоритма поиска КВ достаточно легко строить полидетекторы, осуществляющие обнаружение сразу нескольких типов вирусов. Недостатки программ-детекторов состоят в их неуниверсальности и в запаздывании появления по отношению к новым типам КВ. Это объясняется необходимостью предварительного выделения и исследования КВ с последующим обучением детектора задаче распознавания КВ. Следует учесть также, что некоторые вирусы используют специальные методы противодействия детекторам (фагам). Основной метод противодействия – шифрование кода КВ, затрудняющее его анализ и увеличивающее временные затраты на создание детектора в несколько раз.

Дополнительной мерой противодействия является изменение алгоритма шифрования и ключей от копии к копии, что значительно усложняет процесс выбора эффективной сигнатуры.

Третий метод противодействия программам-детекторам состоит в изменении длины КВ от копии к копии по случайному закону. В результате, настройка большинства из распространенных полидетекторов становится невозможной. Это объясняется тем, что с целью ускорения поиска просматривается не весь файл-вирусоноситель, а лишь определенные его фрагменты с фиксированным смещением от начала или от конца.

Таким образом, использование программ-детекторов эффективно только против известных типов КВ и принципиально невозможно против новых, ранее не известных вирусов.

В отличие от детекторов, просматривающих при поиске КВ все файлы, **программа-вакцина** состыковывается с каждой защищаемой программой подобно вирусу и запоминает ряд ее характеристик.

К эталонным характеристикам, используемым вакцинами, относятся:

- длина программы;
- последовательность машинных кодов в окрестности точки входа в программу;
- контрольная сумма.

Достоинство программ-вакцин состоит в том, что с их помощью можно защищать программы не только от известных, но и новых КВ, так как принцип действия вакцины – фиксация несанкционированных изменений в защищаемой программе, а не поиск какого-либо конкретного КВ.

Именно это обстоятельство является не только преимуществом, но и обуславливает принципиальные недостатки программ-вакцин:

-вакцины не могут обнаружить факт заражения, если оно произошло до момента вакцинации;

-увеличение объема и времени загрузки защищаемых программ.

Основной метод противодействия вакцинам заключается в применении таких КВ, которые не изменяют зафиксированные вакциной характеристики программы. Например, при фиксации признака вирусной атаки по изменению длины программы, КВ могут использовать метод сжатия данных, позволяющий сохранить длину программы неизменной.

Программы-прививки представляют собой отдельный класс программных средств защиты от КВ, реализующих своеобразную “мимикрию”. Принцип действия прививок основан на учете того обстоятельства, что большинство КВ помечают инфицируемые программы каким-либо признаком, чтобы не выполнять их повторное заражение. В противном случае имело бы место многократное инфицирование, сопровождаемое существенным и легко обнаруживаемым увеличением объема зараженных программ. Прививка, не внося никаких других изменений в текст защищаемой программы, помечает ее тем же признаком, что и вирус, который после активизации и проверки наличия указанного признака ошибочно считает программу инфицированной.

Основные преимущества программ-прививок:

-не вносят никаких дополнительных ограничений на работу пользователя и не требуют машинных ресурсов;

-простота в использовании.

Главный недостаток программ-прививок – узкая специализация на определенный тип КВ, поэтому их появление, также как и программ-детекторов, возможно только после тщательного анализа кода КВ.

Кроме того, в ряде случаев использование программ-прививок принципиально невозможно, так как ряд КВ при обнаружении факта заражения всех доступных файлов переходят к фазе активной работы, что может

привести к краху системы.

Использование прививок может быть нейтрализовано за счет разработки новых нестандартных методов индикации факта заражения программы-носителя.

Программы-ревизоры следят за состоянием файловой системы и по принципам работы похожи на программы-вакцины. Ревизоры записывают следующие характеристики исполняемых файлов (программ):

-длину программы;

-контрольную сумму;

-дату и время создания (модификации) файла;

-точку входа в программу.

Отличие их от программ-вакцин состоит в том, что характеристики программ запоминаются в отдельных файлах. Сама проверка (ревизия) также осуществляется отдельной программой. В результате, длины файлов не увеличиваются, и в теле программы никакой дополнительной информации не появляется, что не позволяет КВ определить факт наличия защиты.

Достоинство программ-ревизоров – универсальность. Как и программы-вакцины, ревизоры фиксируют не факт заражения каким-либо конкретным КВ, а любое несанкционированное изменение в файлах программ.

Однако, как и любое средство защиты, программы-ревизоры обладают рядом недостатков:

-эффективность ревизора зависит от частоты его запуска; это означает, что для обеспечения защиты программ и данных необходимо регулярно затрачивать значительное время на просмотр файловой системы; затраты времени зависят от объема информации на дисках, числа просматриваемых файлов, характера проводимых проверок и их качества; поэтому, как показывает опыт практической эксплуатации таких программ, их запуск осуществляется в среднем один-два раза в неделю, что ведет к значительному снижению их эффективности;

-программы-ревизоры не могут обнаружить заражение программы, если оно произошло до момента включения защиты, т. е. они не реагируют на уже зараженные программы;

-применение программ-ревизоров требует от пользователей КСС определенной компьютерной грамотности;

-большинство программ-ревизоров только фиксирует факт модификации программ на диске, не проводя анализа этих изменений; средства анализа и восстановления поврежденных файлов реализованы только для системных файлов.

Основной метод противодействия программам-ревизорам заключается в создании “кочующих” КВ, которые к моменту проверки файла ревизором перемещают код вируса из пораженной программы и возвращают его после проверки.

Мониторы представляют собой резидентные программы, обеспечивающие перехват основных векторов прерываний. При поступлении запроса на обслуживание вектора программа проверяет, не является ли вызываемая функция потенциально опасной для системы, что характерно для КВ (например, форматирование дисков), и запрашивает у пользователей подтверждение на выполнение операций следующих за прерыванием. В случае запрета или отсутствия подтверждения монитор блокирует выполнение пользовательской программы.

Основные недостатки программ-мониторов вытекают из организации ОС. Действия, которые должны отслеживаться монитором для защиты от КВ, по существу являются типичными для штатной работы ОС, так как многие прикладные программы также используют вектора прерываний. Кроме того, каждый системный вызов порождает серию запросов на уровне физической адресации, что может приводить к многочисленным ложным срабатыванием монитора.

Основной путь нейтрализации монитора состоит в обеспечении КВ доступа к функциям ОС, минуя контроль со стороны монитора. Для этого КВ необходимо найти первоначальную точку входа в ОС, устанавливаемую при ее загрузке до включения программ защиты. После того, как значение вектора будет определено, КВ при внедрении в файлы будет использовать именно его, что позволит заблокировать программу-монитор.

Несмотря на такие серьезные недостатки программы-мониторы считаются одним из основных средств защиты от КВ и работы по их совершенствованию ведутся непрерывно.

К **перспективным средствам** защиты относятся универсальные, адаптивные и интеллектуальные антивирусные программы [1 – 3].

Универсальные средства претендуют на блокировку большинства известных типов вирусов. Однако, теоретически подтверждено [8], что множество всех вирусов не перечислимо. Для любого вируса можно создать антивирус, но и для любого средства борьбы с вирусами можно создать вирус, преодолевающий его. Кардинальное решение проблемы антивирусной защиты лежит в создание сред, делающих существование вирусов невозможным.

Адаптивные (самообучающиеся) средства автоматически расширяют список вирусов, которые они блокируют. Это, в первую очередь, программы, содержащие постоянно пополняемые базы вирусов. Наиболее привлекательной выглядит идея создания самообучающегося средства, которое при встрече с неизвестным ему вирусом автоматически анализирует его и добавляет его в свою базу.

Интеллектуальные средства базируются на системах логического вывода. Их суть сводится к определению алгоритма и спецификации программы по ее коду, и выявлению, таким образом, программ, осуществляющих несанкционированные действия. Этот перспективный метод, однако, требует огромных затрат.

Проведенный краткий анализ программных средств защиты показывает, что каждый антивирус способен выявлять и блокировать не все вирусы, а только их ограниченное количество. Разные программы могут "вылечивать" только различные вирусы, по разным авторским алгоритмам и с разной эффективностью блокировки. Поэтому при построении КСАЗ целесообразно использовать комплект антивирусных программ [6 – 7]. Этот комплект должен быть многоуровневым, т. е. обеспечивать N уровней защиты не только против известного количества M вирусов, но против неизвестных новых вирусов. В составе базового четырехуровневого антивирусного комплекта, как показывает практика, целесообразно использовать лучшие полифаги Aidstest Д. Лозинского, Dr. Web И. Данилова, Adinf и Adinf Cure Module (АО Диалог-Наука, Москва), сетевой полифаг Antiviral Toolkit Pro (AVP) Е. Касперского и др.. Данный базовый комплект целесообразно дополнить антивирусными программами ведущих западных стран для повышения вероятности блокирования, прежде всего сетевых и макровирусов.

Недавно в Украине было проведено исследование, направленное на изучение предпочтений отечественных компьютерных пользователей в отношении антивирусных программ [4]. По результатам исследований (рис. 2) видно, что почти пятая часть пользователей (17,94%) вообще не применяют подобные продукты, 43,58% предпочитает антивирусную программу AVP, 19,87% – Norton Antivirus, 12,7% – Dr. Web, 5,91% – используют другие продукты.

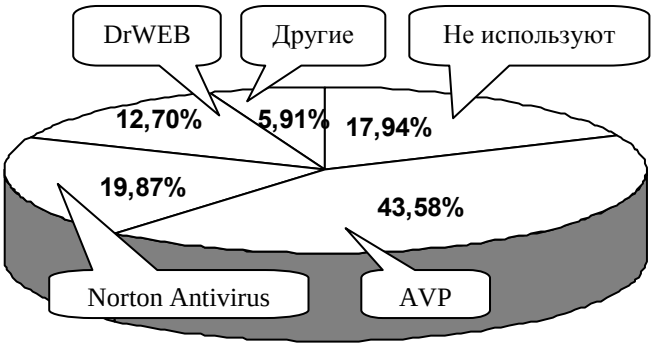

Рисунок 2 – Статистика применения антивирусных программ в Украине

III Выводы

В основе построения современной эффективной КСАЗ должно быть сочетание правовых, организационных и программно-технических методов и механизмов защиты, а также поэтапное устранение отмеченных недостатков в практической реализации указанных составляющих.

*Литература: **1**. Безруков Н. Н. Компьютерная вирусология. Часть 1. Общие принципы функционирования, классификация и каталог наиболее распространенных вирусов. – Киев, КИИГА, 1990. – 150 с. **2**. Барсуков В. С., Водолазкий В. В. Вирусная безопасность / Технологии электронных коммуникаций. Часть 2. Т. 34. – М., 1993. **3**. Левин В. К., Платонов Д. М., Тимофеев Ю. А. Защита информации от компьютерных вирусов / Информационная безопасность компьютерных сетей. Т. 45. – М.: Россия, 1993. **4**. http:/www.crime-research.org.ua - Центр исследования проблем компьютерной преступности. **5**. Уголовный кодекс Украины, 1991 г. **6**. В. В. Шорошев и др. Антивирусная защита вашей ПЭВМ / Бизнес и безопасность, № 6, 1998. **7**. В. Шорошев, А. Ильницький. Класифікація комп'ютерних вірусів і основи захисту від них / Бизнес и безопасность, № 2, 1999. **8**. Зегжда Д. П. и др. Как противостоять вирусной атаке. СПб.: БХВ-Санкт-Петербург, 1995. – 320 с.*