УДК 004.056

А.А. Нечай[1]
П.Е. Котиков [2]

МЕТОДИКА КОМПЛЕКСНОЙ ЗАЩИТЫ ДАННЫХ, ПЕРЕДАВАЕМЫХ И ХРАНИМЫХ НА РАЗЛИЧНЫХ НОСИТЕЛЯХ ИНФОРМАЦИИ

Представленная работа посвящена разработке методики, которая позволяет скрывать данные на носителе, а при угрозе несанкционированного доступа к данной информации гарантированно уничтожать ее, не повреждая носитель.

Значимость полученных результатов заключается в том, что разработанная методика позволяет повысить надежность защиты информации, передаваемой и хранимой как на жестких дисках персональных компьютеров, так и на внешних носителях за счет применения разработанного алгоритма преобразования информации, защиты ее паролем и установки временно́го интервала на доступ к этой информации.

Результаты могут быть использованы в организациях и предприятиях, имеющих дело с большими потоками информации.

Ключевые слова: *защита информации, информационная безопасность, данные, преобразование информации, информационное воздействие, обработка информации, сбор информации.*

A.A. Nechay
P.E. Kotikov

THE METHODOLOGY FOR COMPREHENSIVE PROTECTION OF DATA TRANSMITTED AND STORED ON VARIOUS STORAGE MEDIA

The work deals with the development of a methodology which allows to hide data on the media, and with the threat of unauthorized access to this information is guaranteed to destroy it without damaging the media.

The significance of the findings is that the developed method allows to increase the reliability of protection of the information transmitted and stored on the hard disks of personal computers and external storage media through use of the algorithm of information transformation, protect it with a password and set the time interval for access to this information. The results can be used in organizations and enterprises dealing with large flows of information.

Keywords: *information protection, information security, data, information transformation, information exposure, information processing, information gathering.*

Введение

Возрастающая роль информации в мире обусловливает и выделяет актуальность проблемы информационной безопасности как неотъемлемой составляющей национальной безопасности любого высокоразвитого государства. В Доктрине информационной безопасности Российской Федерации [1] по этому поводу сказано: «Национальная безопасность Российской Федерации существенным образом зависит от информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать».

Роль информации всегда имела огромную значимость в жизни людей, начиная от первобытных племен, выслеживавших добычу и врагов с помощью следопытов, и кончая современными разведывательными комплексами и организациями, поставляющими различные сведения своим ведомствам и правительствам. Ни одно сражение, ни одна операция не обходилась и не обходится без предварительного сбора информации о противостоящей стороне. Любой сделке

[1] Преподаватель Военно-космической академии им. А.Ф. Можайского.

[2] Кандидат технических наук, доцент Военно-космической академии им. А.Ф. Можайского.

в торговле, экономическому договору, любому серьезному мероприятию предшествует тщательный сбор сведений о партнере. Но простой сбор сведений о противнике и партнере раньше никто не называл информационной борьбой. Это называлось разведкой. И этим занимался ограниченный круг лиц, узких профессионалов.

Ситуация резко изменилась с появлением вычислительной техники, коммуникативных каналов и средств массовой информации, имеющих дело с большими потоками информации и затрагивающих интересы огромных масс населения. Современные технические средства ускорили процесс добывания, обработки и доставки информации, процесс ее обновления. Она стала оперативной, глобальной и разноплановой. Информация стала средством воздействия на мысли, поступки, поведение, принимаемые решения, на образ жизни и мировоззрение отдельного человека, коллективов, наций и народов.

Следуя за прогрессом, различные организации, объединения, юридические и даже частные лица применяют средства вычислительной техники для обработки, хранения и передачи данных, затрагивающих все сферы их жизнедеятельности и не предназначенных для третьих лиц. С развитием вычислительной техники стали развивать и способы воздействия на неё [2]. В связи с этим огромное значение получает такой показатель передачи и хранения данных, как безопасность. Развитие способов несанкционированного доступа к информации ограниченного доступа поднимает на высокий уровень актуальность безопасного хранения и передачи данных.

Целью работы является повышение надежности защиты информации, передаваемой и хранимой как на жестких дисках персональных компьютеров, так и на внешних носителях за счет применения разработанной методики преобразования информации, защиты ее паролем и установки временно́го интервала на доступ к этой информации.

Результатом решения поставленной цели стал программный комплекс, который позволяет скрывать данные на носителе, а при угрозе несанкционированного доступа к данной информации гарантированно уничтожать ее, не повреждая носитель.

1. Постановка задачи

В автоматизированных системах специального назначения широкое применение находят типовые средства защиты информации известных производителей, что ведет к увеличению активности злоумышленников по поиску в них уязвимостей. Если использование одного средства защиты недостаточно снижает риски несанкционированного доступа к информации, то применяются дополнительные решения, которые состоят из различных элементов защиты информации.

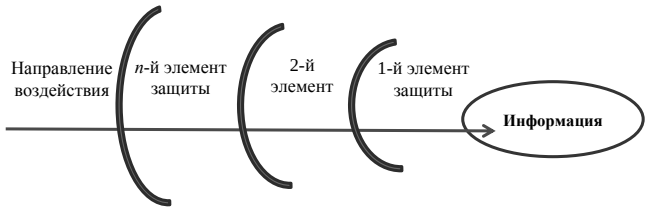

Рис. 1. Структура защищаемого объекта, обрабатывающего информацию

На рис. 1 представлена структурная схема объекта, состоящего из n элементов защиты информации от несанкционированного доступа. В связи с повышенным спросом к надежности защиты информации сформулируем нижеприведенную задачу.

Дано: 1. Объект, обрабатывающий информацию, на котором установлено три штатных элемента защиты. Первый элемент защиты включает в себя межсетевой экран, второй элемент – прокси-сервер (Proxy-Server), третий уровень – виртуальная частная сеть (VPN).

2. Количество преодолений уровней защиты информации в единицу времени = 3,5.

Необходимо: разработать комплексный метод защиты данных, дополняющий штатные уровни защиты информации и обеспечивающий вероятность защищенности информации $P_{\text{защ}} = 0{,}9$.

Ограничения: поток событий обладает свойствами стационарности, отсутствия последействия и ординарности.

Обозначим λ количество преодолений уровней защиты информации в единицу времени t. Для упрощения модели будем считать, что для одного уровня защиты информации поток событий обладает свойствами стационарности, отсутствия последействия и ординарности. Событие преодоления одного уровня защиты зависит только от длины временного промежутка, в течение которого приходится обрабатывать данные. Событие преодоления одного уровня защиты не зависит в любом промежутке времени от того, появлялись события в прошлом или нет. Появление более одного события за малый промежуток времени практически невозможно.

Вероятность того, что произойдет преодоление n уровней защиты, будет определяться как

$$P(n) = \frac{(\lambda t)^n}{n!} e^{-\lambda t}$$

Пример 1. Произведем расчеты вероятности защищенности информации при трех элементах защиты:

$\lambda = 3{,}5$;

$t = 1$ сек.;

$n = 3$.

Получаем: $P(3) = 0{,}2157854690$ – вероятность преодоления 3-х элементов защиты, следовательно, вероятность защищенности информации при установленных 3-х элементах защиты примет следующее значение:

$P_{защ} = 1 - P(n) = 1 - 0{,}2157854690 = 0{,}784214531$.

Вероятность защищенности информации $P_{защ}$ при трех элементах защиты не удовлетворяет поставленной задаче, так как заданная вероятность – 0,9, в связи с этим повышается актуальность разработки и внедрения программного комплекса, реализующего дополнительные элементы защиты.

Разработанная методика позволяет добавить к уже существующим элементам следующие элементы защиты информации:

1) криптографическую защиту информации, позволяющую скрывать файл с данными посредством разработанного алгоритма преобразования данных;

2) защиту паролем доступа к файлу;

3) временной интервал разрешенной работы с файлом;

4) систему гарантированного уничтожения информации при несанкционированном доступе к файлу, а также при превышении разрешенного времени работы с файлом.

Добавление дополнительных элементов защиты существенно повышает надежность защиты информации. Докажем это путем расчета вероятности защищенности информации, рассчитав ее совместно с добавленными четырьмя элементами к трем базовым элементам защиты.

Пример 2. Произведем расчеты вероятности защищенности информации для семи элементов защиты:

$\lambda = 3{,}5$;

$t = 1$ сек.;

$n = 7$.

Получаем: $P(3) = 0{,}0385491749$ – вероятность преодоления 7-ми элементов защиты, следовательно, вероятность защищенности информации при установленных 7-ми элементах защиты информации примет следующее значение:

$P_{защ} = 1 - P(n) = 1 - 0{,}0385491749 = 0{,}9614508251$.

Вероятность защищенности информации $P_{защ}$ при семи элементах защиты удовлетворяет поставленной задаче, так как полученная вероятность превышает заданный порог в 0,9.

Приведем график зависимости вероятности преодоления элементов защиты информации от количества элементов защиты (рис. 2).

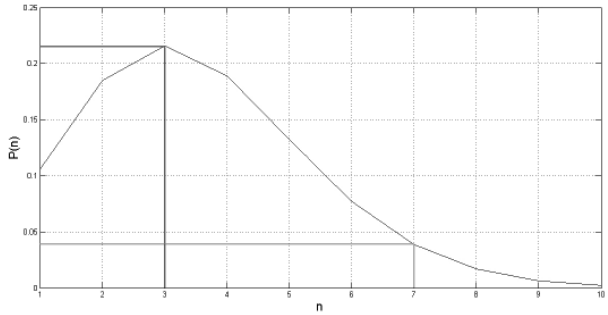

Рис. 2. Зависимости *P(n)* – вероятности преодоления элементов защиты информации от *n* – количества элементов защиты

Выводы. Применение дополнительных элементов защиты увеличивает надежность защиты информации и позволяет уменьшить вероятность преодоления дополнительных элементов защиты за определенное время. Это снижает риск несанкционированного доступа к информации.

Из расчетов следует, что разработанная методика комплексной защиты данных позволяет на 18% увеличить вероятность защищенности информации.

Цель разработки методики комплексной защиты данных, передаваемых и хранимых на различных носителях информации, достигнута. Полученное значение защищенности превышает заданное, что, в свою очередь, благоприятно скажется на надежности защиты информации.

Литература

1. Лохвицкий В.А. Подход к построению системы автоматизированной интеграции информации в базу данных для её своевременной актуализации / В.А. Лохвицкий, С.В. Калиниченко, А.А. Нечай // Мир современной науки. – 2014. – № 2 (24). – С. 8–12.

2. Нечай А.А. Выявление недекларированных возможностей аппаратно-программного обеспечения / А.А. Нечай // Экономика и социум. – 2014. – № 1–2 (10). – С. 457–460.

3. Нечай А.А. Специфика проявления уязвимостей в автоматизированных системах управления критически важными объектами / А.А. Нечай, П.Е. Котиков // Современные тенденции в образовании и науке : сборник научных трудов по материалам Международной научно-практической конференции : в 14 ч. – Тамбов, 2014. – С. 96–97.

4. Вепрев С.Б. Скрытый метод выявления утечек инсайдерской информации / С.Б. Вепрев, П.И. Гончаров // Вестник Российского нового университета. – 2014. – № 4. – С. 152–155.