УДК 004.056.53
ББК 32.973.26-018.2
К 57

Коджешау М.А.
Кандидат педагогических наук, доцент кафедры прикладной математики, информационных технологий и информационной безопасности факультета математики и компьютерных Адыгейского государственного университета, Майкоп, тел. (8772) 593904, e-mail: marina_70@mail.ru

Технологии и алгоритмы информационной безопасности

(Рецензирована)

Аннотация. *Рассмотрены методы защиты информационных систем от несанкционированного доступа. Приведена классификация алгоритмов шифрования, используемых для защиты данных, и рассмотрены методы защиты на примере операционных систем разных поколений и в программном обеспечении на примере операционных систем. Особое внимание уделено актуальной на современном этапе развития информационных технологий безопасности и защите данных в компьютерных сетях.*

Ключевые слова: *криптография, алгоритм шифрования, шифровка, шифрование, информационная система, уровень информационной безопасности, несанкционированный доступ.*

Kodzheshau M.A.
Candidate of Pedagogy, Associate Professor of Department of Applied Mathematics, Information Technologies and Information Security of the Mathematics and Computer Science Faculty, Adyghe State University, Maikop, ph. (8772) 593904, e-mail: marina_70@mail.ru

Technologies and algorithms of information security

Abstract. *The paper explores methods of protection of information systems against unauthorized access. Classification of encryption algorithms used for data protection is given. Protection methods are examined using operating systems of different generations and operating systems in the software as an example. Special attention is paid to information security and data protection in computer networks, relevant at the present stage of development of information technologies.*

Keywords: *cryptography, encryption algorithm, encryption, enciphering, information system, level of information security, unauthorized access.*

Любая информационная система (ИС) должна соответствовать трем основным требованиям: функциональность, информационная безопасность, совместимость. Рассмотрим основные положения, связанные с информационной безопасностью ИС.

Присвоение категорий безопасности информации и информационным системам производится на основе оценки ущерба, который может быть нанесен нарушениями безопасности. При этом выделяют три аспекта информационной безопасности: доступность, конфиденциальность и целостность [1].

Современные информационные технологии и методы криптографической защиты предлагают множество различных решений проблемы безопасности конфиденциальной информации, основанных на тех или иных механизмах, в зависимости от ситуации и условий, смещенных в сторону того или иного составляющего вектора. Значительное количество публикаций по рассматриваемой тематике, их анализ в отечественных и зарубежных изданиях подчеркивают значимость и актуальность рассматриваемого вопроса [2–5]. Для определения оптимального уровня информационной безопасности системы необходимо учитывать степень взаимодействия всех ее составляющих (рис. 1) и влияние их на работу конечного пользователя с учетом применимости того или иного решения в конкретной ситуации функционирования информационной системы.

В процессе разработки системы защиты информационной системы необходим учет того, что целью реализации угроз является нарушение определенных для объекта характеристик безопасности (конфиденциальность, целостность, доступность) или создание условий для их нарушения. К подобным нарушениям можно отнести: несанкционированное ознакомление, модификация и блокировка целевой информации, хранимой и обрабатываемой в информационной системе; несанкционированное ознакомление с файлами конфигурации и на-

стройками средств защиты информации; несанкционированное изменение конфигурационных файлов и настроек средств защиты информации; нарушение режимов функционирования программно-технических средств информационной системы и изменение функциональных элементов и их корректной реакции на соответствующую операцию.

Рис. 1. Уровни обеспечения ИБ

При рассмотрении проблем защиты данных, например, в компьютерных сетях, прежде всего, возникает вопрос о классификации сбоев и нарушений прав доступа, которые могут привести к уничтожению или нежелательной модификации данных.

Среди таких потенциальных «угроз» можно выделить: сбои оборудования (сбои кабельной системы, перебои электропитания, сбои дисковых систем, сбои систем архивации данных); потери информации из-за некорректной работы программного обеспечения (ПО) (сбои работы серверов, рабочих станций, сетевых карт и т.д., потеря или изменение данных при ошибках ПО); потери, связанные с несанкционированным доступом (потери при заражении системы компьютерными вирусами, несанкционированное копирование, уничтожение или подделка информации); потери информации, связанные с неправильным хранением архивных данных; ошибки обслуживающего персонала и пользователей.

В настоящее время разработана целая система алгоритмов шифрования, призванных обеспечить надежную защиту на всех уровнях функционирования информационных систем (рис. 2):

- симметричные (с секретным, единым ключом, одноключевые, single-key). К ним относятся: *потоковые* (шифрование потока данных): с одноразовым или бесконечным ключом (infinite-key cipher); с конечным ключом (система Вернама – Vernam); на основе генератора псевдослучайных чисел (ПСЧ); *блочные* (шифрование данных поблочно): шифры перестановки (permutation, P-блоки) и шифры замены (подстановки, substitution, S-блоки) – моноал-

фавитные (код Цезаря) и полиалфавитные (шифр Видженера, цилиндр Джефферсона, диск Уэтстоуна, Enigma); составные;

- асимметричные (с открытым ключом, public-key): Диффи-Хеллман DH (Diffie, Hellman); Райвест-Шамир-Адлеман RSA (Rivest, Shamir, Adleman); Эль-Гамаль (ElGamal).

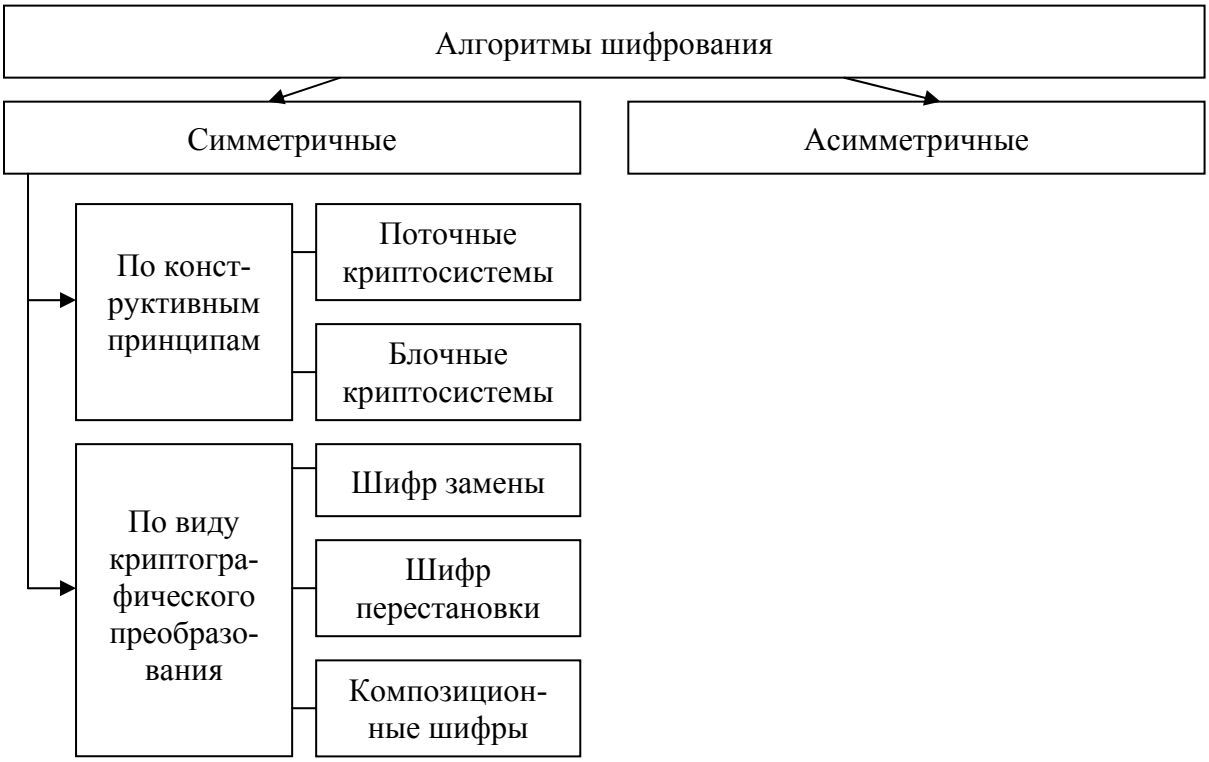

Рис. 2. Классификация алгоритмов шифрования

Кроме того, есть разделение алгоритмов шифрования на собственно шифры (ciphers) и коды (codes). Шифры работают с отдельными битами, буквами, символами. Коды оперируют лингвистическими элементами (слоги, слова, фразы) [6].

Наряду с алгоритмами шифрования значительное место в разработке системы защиты занимают и методы защиты. Рассмотрим программные и программно-аппаратные методы защиты. Операционная система является важнейшим программным компонентом любой вычислительной машины, поэтому от уровня реализации политики безопасности в каждой конкретной ОС во многом зависит и общая безопасность информационной системы. Безопасность ОС – это состояние ОС, при котором невозможно случайное или преднамеренное нарушение ее функционирования, а также нарушение безопасности находящихся под управлением ОС ресурсов системы. К особенностям ОС, которые позволяют выделить вопросы обеспечения ее безопасности в особую категорию, относятся: управление всеми ресурсами системы; наличие встроенных механизмов, которые прямо или косвенно влияют на безопасность программ и данных, работающих в среде ОС; обеспечение интерфейса пользователя с ресурсами системы; размеры и сложность ОС.

Большинство ОС обладают дефектами с точки зрения обеспечения безопасности данных в системе, что обусловлено выполнением задачи обеспечения максимальной доступности системы для пользователя.

Основной проблемой обеспечения безопасности ОС является проблема создания механизмов контроля доступа к ресурсам системы. Процедура контроля доступа заключается в проверке соответствия запроса субъекта предоставленным ему правам доступа к ресурсам. Кроме того, ОС содержит вспомогательные средства защиты, такие как средства мониторинга, профилактического контроля и аудита. В совокупности механизмы контроля доступа и вспомогательные средства защиты образуют механизмы управления доступом.

Нельзя не отметить особенности шифрованных архивов. Программы-архиваторы, как правило, имеют опцию шифровки. Ею можно пользоваться для не слишком важной информации, так как используемые там методы шифровки не слишком надежны (подчиняются официальным экспортным ограничениям). Все это не позволяет всерьез рассчитывать на безукоризненную защиту. Из числа наиболее современных криптографических алгоритмов можно выделить 3DES, IDEA, Blowfish, Cast-128 и некоторые из AES, включая новый AES Rijndael наряду с ZIP-сжатием. Что касается методов шифрования, реализованных в современных программах-архиваторах, то здесь выбор более ограничен. В большинстве случаев в конкретном архиваторе (речь идет о популярных архиваторах) реализован какой-нибудь один метод. Кроме этого стандартное ZIP-кодирование не относится сегодня к числу надежных, равно как и шифрование с применением алгоритма DES [7].

Современный 64-битный блочный шифр Blowfish с ключом переменной длины от 32 до 48 бит в настоящее время считается достаточно сильным алгоритмом. Он был разработан в 1993 году в качестве замены уже существующих алгоритмов и является намного более быстрым, чем DES, Triple DES и IDEA. Но наиболее надежным сегодня считается Rijndael – новый стандарт шифрования AES, принятый США в 2001 году. AES имеет три размера ключа: 128, 192 и 256 бит и обладает массой достоинств. К их числу относятся: высокая скорость шифрования; минимальные требования к вычислительным ресурсам; устойчивость против всех известных атак и легкая расширяемость (при необходимости можно увеличить размер блока или ключа шифрования). Более того, в ближайшем будущем AES Rijndael останется самым надежным методом, поскольку даже если предположить, что появится компьютер, способный опробовать 255 ключей в секунду, то потребуется приблизительно 149 триллионов лет, чтобы определить 128-битный ключ AES [7].

Шифрование в программном обеспечении можно рассмотреть на примере MS Office. Фирма Майкрософт включила в свои продукты некоторое подобие криптозащиты. Но алгоритм шифровки не описан, что, как известно, является показателем ненадежности. Кроме того, имеются данные, что Майкрософт оставляет в используемых криптоалгоритмах «черный ход». Если вам очень нужно расшифровать файл, пароль к которому утрачен, можно обратиться в фирму. По официальному запросу, при достаточных основаниях они проводят расшифровку файлов Word и Excel. Если у стороннего пользователя возникает желание внедрить в программу шифрования «черный ход», то действия разработчика заключаются в том, что в каждый заголовок, помимо перечисленной выше информации, записывается еще и файловый ключ, зашифрованный на некотором «универсальном ключе» (всего-то 32 байта лишней информации). Это уравнивает в возможностях расшифрования информации легальных пользователей и владельцев данного спецключа.

Примером может служить файловая система EFS (Encrypting File System), появившаяся в свое время в Microsoft Windows 2000, осуществлявшая прозрачное шифрование файлов. Шифрование выполняется на случайном файловом ключе (FEK – File Encryption Key), который зашифровывается асимметричным алгоритмом на открытом ключе пользователя и хранится вместе с зашифрованным файлом. Кроме этого FEK зашифровывается и на одном или нескольких открытых ключах агентов восстановления данных и также записывается в файловый дескриптор. Таким образом, агент восстановления данных может в любой момент расшифровать файл с помощью своего секретного ключа. Данная схема представляет собой реальный пример использования «черного хода» – зашифрованная пользователем информация в любой момент может быть получена, например, администрацией организации, в которой он работает [8].

Алгоритмы шифрования, доступные в Office 2010, зависят от алгоритмов, доступ к которым осуществляется через интерфейс API в ОС Windows. Office 2010 кроме Cryptography API (CryptoAPI) также поддерживает интерфейс CNG (CryptoAPI: Next Generation), поддерживающий модули шифрования сторонних производителей. В Office 2010 и Office 2007 с пакетом обновления 2 (SP2) используются следующие алгоритмы шифрования CNG и другие криптографические расширения CNG, установленные в систе-

ме: AES, DES, DESX, 3DES, 3DES_112 и RC2, а также алгоритмы хэширования CNG и другие криптографические расширения CNG: MD2, MD4, MD5, RIPEMD-128, RIPEMD-160, SHA-1, SHA256, SHA384 и SHA512.

Шифрование – достаточно надежный метод также и для защиты информации на жестком диске. Однако если количество закрываемой информации не исчерпывается двумя-тремя файлами, то пользователю будет несколько сложно с ней работать: каждый раз нужно будет файлы расшифровывать, а после редактирования – зашифровывать обратно. При этом на диске могут остаться страховочные копии файлов, которые создают многие редакторы. Поэтому удобно использовать специальные программы (драйверы), которые автоматически зашифровывают и расшифровывают всю информацию при записи ее на диск и чтении с диска.

Проблема защиты информации от несанкционированного доступа особо обострилась с широким распространением локальных и особенно глобальных компьютерных сетей. Необходимо также отметить, что зачастую ущерб наносится не из-за «злого умысла», а из-за элементарных ошибок пользователей, которые случайно портят или удаляют жизненно важные данные. В связи с этим, помимо контроля доступа, необходимым элементом защиты информации в компьютерных сетях является разграничение полномочий пользователей.

В компьютерных сетях при организации контроля доступа и разграничения полномочий пользователей чаще всего используются встроенные средства сетевых операционных систем. Но в такой системе организации защиты все равно остается слабое место: уровень доступа и возможность входа в систему определяются паролем. Для исключения возможности неавторизованного входа в компьютерную сеть в последнее время используется комбинированный подход – пароль+идентификация пользователя по персональному «ключу». В качестве «ключа» может использоваться пластиковая карта (магнитная или со встроенной микросхемой – смарт-карточка) или различные устройства для идентификации личности по биометрической информации – по радужной оболочке глаза или отпечаткам пальцев, размерам кисти руки и т.д.

Оснастив сервер или сетевые рабочие станции, например, устройством чтения смарт-карточек и специальным программным обеспечением, можно значительно повысить степень защиты от несанкционированного доступа. В этом случае для доступа к компьютеру пользователь должен вставить смарт-карту в устройство чтения и ввести свой персональный код. Программное обеспечение позволяет установить несколько уровней безопасности, которые управляются системным администратором. Возможен и комбинированный подход с вводом дополнительного пароля, при этом приняты специальные меры против «перехвата» пароля с клавиатуры. Этот подход значительно надежнее применения паролей, поскольку, если пароль подглядели, пользователь об этом может не знать, если же пропала карточка, можно принять меры немедленно. Смарт-карты управления доступом позволяют реализовать, в частности, такие функции, как контроль входа, доступ к устройствам персонального компьютера, доступ к программам, файлам и командам.

Защита информации при удаленном доступе. По мере расширения деятельности предприятий, роста численности персонала и появления новых филиалов возникает необходимость доступа удаленных пользователей (или групп пользователей) к вычислительным и информационным ресурсам главного офиса компаний. В связи с этим защита информации, передаваемой по каналам удаленного доступа, требует особого подхода.

В частности, в мостах и маршрутизаторах удаленного доступа применяется сегментация пакетов – их разделение и передача параллельно по двум линиям, – что делает невозможным «перехват» данных при незаконном подключении «хакера» к одной из линий. К тому же используемая при передаче данных процедура сжатия передаваемых пакетов гарантирует невозможность расшифровки «перехваченных» данных. Кроме того, мосты и маршрутизаторы удаленного доступа могут быть запрограммированы таким образом, что удаленные пользователи будут ограничены в доступе к отдельным ресурсам сети главного офиса.

Разработаны и специальные устройства контроля доступа к компьютерным сетям по коммутируемым линиям. Например, фирмой AT&T еще в 1995 году был предложен модуль

Remote Port Security Device (PRSD), представляющий собой два блока размером с обычный модем: RPSD Lock (замок), устанавливаемый в центральном офисе, и RPSD Key (ключ), подключаемый к модему удаленного пользователя. RPSD Key и Lock позволяют установить несколько уровней защиты и контроля доступа, в частности: рабочих мест (work location subsystem) и шифрование данных, передаваемых по линии при помощи генерируемых цифровых ключей. В настоящее время ассортимент предлагаемых на рынке приложений для ограничения доступа достаточно широк и охватывает разноплановые программные продукты. Одни из них блокируют доступ к настройкам операционной системы, другие – позволяют контролировать доступ к разнообразным устройствам, третьи – полностью блокируют компьютер в отсутствии пользователя, четвертые – обеспечивают скрытие персональных данных. Нередко указанные возможности сочетаются в той или иной комбинации, что вполне понятно, ведь многим пользователям для решения стоящих перед ними задач требуется ограничить доступ сразу по нескольким направлениям.

Таким образом, выбор для конкретных информационных систем должен быть основан на глубоком анализе слабых и сильных сторон тех или иных методов защиты. Обоснованный выбор той или иной системы защиты, в общем-то, должен опираться на какие-то критерии эффективности. К сожалению, до сих пор не разработаны подходящие методики оценки эффективности криптографических систем.

Наиболее простой критерий такой эффективности – вероятность раскрытия ключа или мощность множества ключей, иначе говоря, криптостойкость. Для ее численной оценки можно использовать также и сложность раскрытия шифра путем перебора всех ключей. Но в этой схеме есть ряд недостатков, определяющихся тем, что этот критерий не учитывает важных требований к криптосистемам: невозможность раскрытия или осмысленной модификации информации на основе анализа ее структуры; совершенство используемых протоколов защиты; минимальный объем используемой ключевой информации; минимальная сложность реализации (в количестве машинных операций), ее стоимость; высокая оперативность.

На основе проведенного анализа уровня развития и сформированности систем информационной безопасности в России и за рубежом можно сделать определенные выводы. В настоящее время развиваются не только технологии информационной безопасности, но и технологии, которые могут осуществлять различные правонарушения даже в защищенной системе [5, 9]. Таким образом, любая система обеспечения ИБ, являясь в некотором смысле надежной, не дает полного обеспечения безопасности. Именно поэтому необходимо вести исследования в этой сфере, осуществляя комплекный подход при конструировании систем защиты информации, используя не только проверенные технологии и устройства, но и персонал, который обучен и компетентен в области технологий и права.

Примечания:

1. Галатенко В.А. Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности // Jet Info. 2008. № 4. URL: http://www.jetinfo.ru/stati/kategorirovanie-informatsii-i-informatsionnykh-sistem-obespechenie-bazovogo-urovnya-informatsionnoj ИТ-ПОРТАЛ КОМПАНИИ «ИНФОСИСТЕМЫ ДЖЕТ».
2. Fuchs L. Roles in information security – A survey and classification of the research area // Computers & Security. 2011. Vol. 30, Iss. 8. P. 748–769. URL: https://doi.org/10.1016/j.cose.2011.08.002
3. Брюхомицкий Ю.А., Макаревич О.Б. Обзор исследований и разработок по информационной безопасности. По материалам докладов XII Междунар. науч.-практ. конф. «Информационная безопасность – 2012» // Известия ЮФУ. Технические науки. 2012. С. 8–21.
4. Брюхомицкий Ю.А., Макаревич О.Б. Обзор иссле-

References:

1. Galatenko V.A. Categorization of information and information systems. Provision of the basic level of information security // Jet Info. 2008. No. 4. URL: http://www.jetinfo.ru/stati/kategorirovanie-informatsii-i-informatsionnykh-sistem-obespechenie-bazovogo-urovnya-informatsionnoj IT PORTAL OF “INFOSYSTEMS JET” COMPANY.
2. Fuchs L. Roles in information security – A survey and classification of the research area // Computers & Security. 2011. Vol. 30, Iss. 8. P. 748–769. URL: https://doi.org/10.1016/j.cose.2011.08.002
3. Bryukhomitsky Yu.A., Makarevich O.B. Review of research and development on information security. Based on the reports of the 12th International scient. and pract. conf. “Information security – 2012” // News of SFedU. Technical Sciences. 2012. P. 8–21.
4. Bryukhomitsky Yu.A., Makarevich O.B. Review of

дований и разработок по информационной безопасности. По материалам докладов XIII Междунар. науч.-практ. конф. «Информационная безопасность – 2013» // Известия ЮФУ. Технические науки. 2013. № 12. С. 7–25.

5. Арутюнов В.В. Современные проблемы и задачи обеспечения информационной безопасности // Вестник Московского финансово-юридического университета. 2016. № 2. С. 213–222.
6. Чмора А.Л. Современная прикладная криптография. 2-е изд., стер. М.: Гелиос АРВ, 2004. 256 с.
7. Шляхтина С. Архиваторы помогают защищать информацию. URL: http://compress.ru/article.aspx?id=10696
8. Зубанов Ф.В. Microsoft Windows 2000. Планирование, развертывание, установка. 2-е изд. М.: Рус. редакция, 2000. 592 с.
9. Усцелемов В.Н. Совершенствование подсистемы информационной безопасности на основе интеллектуальных технологий // Прикладная информатика. 2016. Т. 11, № 3 (63). С. 31–38.

research and development on information security. Based on the reports of the 13th Int. scient. and pract. conf. “Information security – 2013” // News of SFedU. Technical Sciences. No. 123. P. 7–25.

5. Arutyunov V.V. Contemporary problems and tasks of ensuring information security // Bulletin of Moscow University of Finance and Law. 2016. No. 2. P. 213–222.
6. Chmora A.L. Modern Applied Cryptography. 2nd ed., ster. M.: Gelios ARV, 2004. 256 pp.
7. Shlyakhtina S. Archivers help to protect information. URL: http://compress.ru/article.aspx?id=10696
8. Zubanov F.V. Microsoft Windows 2000. Planning, deployment, installation. 2nd ed. M.: Rus. Edition, 2000. 592 pp.
9. Ustselemov V.N. Improvement of the information security subsystem based on intellectual technologies // Applied Informatics. 2016. Vol. 11, No. 3 (63). P. 31-38.