УДК 004.7

DOI: 10.17748/2075-9908.2015.7.3.184-189

ГАЛАШИНА Надежда Евгеньевна,
преподаватель кафедры

GALASHINA Nadezhda Evgenyevna,
Lecturer of Chair

КОСТЕЖ Владимир Александрович,
кандидат технических наук, доцент

KOSTEZH Vladimir Alexandrovich,
Candidate of Technical Sciences, Associate Professor,

ЛЕВКОВЕЦ Леонид Борисович,
кандидат технических наук, доцент

LEVKOVETS Leonid Borisovich,
Candidate of Technical Sciences, Professor

**ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ
ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ С
ИСПОЛЬЗОВАНИЕМ ВАРИАБЕЛЬНЫХ ПО
СОСТАВУ СРЕДСТВ**

**TECHNOLOGY ENSURING PROTECTION OF
COMPUTER NETWORKS USING THE MEANS
VARIABLE IN COMPOSITION**

В статье описана зависимость устойчивой работы вычислительной сети от целенаправленных изменений режимов функционирования программно-аппаратных средств. Рассмотрены технологии обеспечения защиты вычислительных сетей с использованием средств, переменных по времени, а также средств, переменных по номенклатуре. Практически отработан вариант структуры технологии обеспечения защиты вычислительных сетей с использованием программных средств, сочетающихся по номенклатуре. Для проверки методик практической реализации номенклатурного метода защиты с использованием двух программ шифрования BitLocker и TrueCrypt использовалась программа виртуализации VMware Workstation 11 с установленной операционной системой Microsoft Windows 7 Enterprise без доверенного платформенного модуля.

The article describes the dependence of steady operation of computer network on a deliberate change of operation modes of software and hardware.

The authors consider the technologies ensuring computer network security with the use of the means variable in time and with the use of the means variable in nomenclature. Structure of the technology ensuring protection of computer networks using the softwares compatible in nomenclature has been worked through.

To verify the practical implementation of the nomenclature method using two programs BitLocker and TrueCrypt was used the virtualization program VMware Workstation 11 with the operating system Microsoft Windows 7 Enterprise without a TPM.

Ключевые слова: защита информации; социальные проблемы защиты информации; несанкционированный доступ; шифрование; компьютерные сети; рабочие станции; переменные средства; программно-аппаратные средства; пароль; ключ доступа.

Keywords: information security; social issues of information security; unauthorized access; encryption; computer network; workstations; flexible tools; software and hardware; password; access key.

Защита информации носит как исторические, так и социальные аспекты. Известно, что еще с древних времен люди стремились сохранить важную информацию. Так, достоверно известно, что первым, кто шифровал информацию для своих подчиненных, был император Гай Юлий Цезарь. Для этой цели он использовал простой, но довольно эффективный способ, в котором каждая буква текста заменялась буквой алфавита, расположенной на постоянном расстоянии от кодируемой буквы.

В дальнейшем предупреждение несанкционированного доступа к информации сводилось к использованию паролей, регламентирующих право доступа пользователя к определенной части информации. Конечно, это не решало всей проблемы защиты, но затрудняло злоумышленникам быстрый доступ к информации.

С развитием вычислительной техники и существенного увеличения хранимой и передаваемой информации начали разрабатываться комплексные методы защиты, включающие технические средства, организационные мероприятия и методы криптографии. Для их реализации были разработаны многочисленные теоретические подходы и практические реализации [2].

Важность шифрования информации и ее взлома особенно проявилась во время Второй мировой войны, когда были разработаны сложнейшие шифровальные и дешифровальные машины, которые определяли успех проведения многих важнейших военных операций.

В настоящее время вершиной защиты «гражданской» информации является использование электронных денег, для реализации алгоритма которых разработаны протоколы шифрования и электронной подписи.

Основная проблема предотвращения взлома состоит в использовании злоумышленниками автоматических средств, работающих с очень большой скоростью и посылающих колоссальное количество запросов. По статистике, утечка коммерческой информации в 60 случаях из 100 приводит к банкротству фирмы. Поэтому многие иностранные компании вкладывают до 40% средств от прибыли в информационную безопасность своего предприятия. По некоторым данным, 92% всех взломов остаются неразглашенными, так как информация о взломе может нанести огромный ущерб репутации пострадавшего предприятия.

С точки зрения социальных проблем защита информации регламентирует неприкосновенность собственности и неприкосновенность переписки [1]. Целью защиты являются: предотвращение утечки, хищения, утраты, подделки информации; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

В настоящее время основой компьютерных технологий является корпоративная сеть, в большинстве случаев подключенная к Интернету. Для защиты корпоративных информационных сетей такого типа используется брандмауэр (дословно «противопожарная стена»). Брандмауэр представляет собой программный или аппаратный комплекс, который проверяет данные, входящие через Интернет или сеть, и в зависимости от параметров брандмауэра блокирует или разрешает их передачу на компьютер.

Кроме создания новых технических средств защиты информации, широко разрабатываются новые теоретические подходы. Так, одним из направлений являются стеганографические технологии [3], основанные на клептографии, пост-квантовой криптографии и некриптографических подходах.

В работе [4] показаны способы применения гомоморфных преобразований при проектировании и анализе защищенных компьютерных систем. Раскрыты общие принципы применения алгебраических систем для исследования защищенности и построения моделей безопасности.

Работа [5] посвящена фундаментальному решению задачи оптимизации процесса защиты дискретной информации с позиций виртуализации информационных потоков.

В нашей статье описываются используемые нами способы защиты вычислительных сетей с помощью шифрования информации, хранящейся на компьютере. Для проверки методик практической реализации номенклатурного метода защиты с использованием двух программ шифрования BitLocker и TrueCrypt [8] использовалась программа виртуализации VMware Workstation 11 с установленной операционной системой Microsoft Windows 7 Enterprise без доверенного платформенного модуля. Данный метод защиты можно назвать эшелонированным, гибридным или комбинированным.

При этом структуру защиты можно описать следующим образом:

A – множество, включающее средства для защиты вычислительных сетей.

В качестве примера рассмотрен определенный состав средств защиты вычислительных сетей.

$a_n \in A$,

$n = 1, \dots, d$

a_n – элемент множества средств, используемый для защиты вычислительной сети;

d – количество используемых в конкретном случае средств защиты вычислительных сетей.

Рассмотрены:

a_1 – штатное средство шифрования операционных систем Microsoft Windows BitLocker [6];

a_2 – штатное средство архивации операционных систем Microsoft Windows [6], [7];

a_3 – сторонне средство шифрования TrueCrypt [8];

a_4 – сторонне средство архивации Acronis True Image [9];

a_2, a_4 используются в традиционном режиме, в соответствии с инструкциями администраторов вычислительной сети.

T – множество дискретных промежутков времени использования средств защиты;

t_n – дискретный промежуток времени использования средства a_n ;

$t_n \in T$;

$n = 1, \dots, d$;

t_1 – расписание использования средства a_1 ;

C – множество сочетаний по времени и номенклатуре средств защиты вычислительных сетей.

$\{a_1, t_1\}, \{a_2, t_2\}, \{a_3, t_3\}, \{a_4, t_4\} \in C$

Технология обеспечения защиты вычислительных сетей с использованием средств, переменных по времени

Данная технология основывается на смене средств защиты по определенной закономерности, а именно – регулярной смене средств защиты по времени.

Использование различных криптографических средств защиты информации в разное время повышает уровень неопределенности для атакующего. Например, в определенный момент времени информация передается с использованием симметричного алгоритма шифрова-

ния, в другой момент времени – ассиметричным методом шифрования. Либо в определенное время используется один алгоритм ассиметричного шифрования, в другой момент – иной алгоритм ассиметричного шифрования. Данный способ является более продуктивным, так как не требует дополнительной защиты канала связи в случае использования симметричного метода шифрования.

В случае использования такого метода защиты для злоумышленника создаются дополнительные барьеры, препятствующие атаке на конфиденциальную информацию, а именно дополнительное время:

- на подбор необходимой криптосистемы;
- на подбор криптографического алгоритма;
- на новую разработку и реализацию алгоритма перебора ключей для иной криптосистемы.

Таким образом, организационными методами увеличиваются затраты атакующего.

Технология обеспечения защиты вычислительных сетей с использованием средств, переменных по номенклатуре

Данная технология защиты включает использование двух методов защиты в один и тот же момент времени. Данный метод защиты иначе можно назвать эшелонированным, гибридным или комбинированным.

Если определенные угрозы и уязвимости настолько велики, что одно типовое решение недостаточно снижает риски, то приходится внедрять два-три решения различных разработчиков, каждый из которых использует свою типовую технологию.

На практике отработан вариант технологической структуры обеспечения защиты вычислительных сетей с использованием средств, сочетающихся по номенклатуре.

Для проверки методик практической реализации номенклатурного метода защиты с использованием двух программ шифрования BitLocker [6] и TrueCrypt использовалась программа виртуализации VMware Workstation 11 с установленной операционной системой Microsoft Windows 7 Enterprise без доверенного платформенного модуля.

Для практической реализации номенклатурного метода защиты с использованием двух программ шифрования BitLocker и TrueCrypt программа виртуализации не требуется.

Технология BitLocker является штатным средством шифрования операционных систем Microsoft Vista, 7, 8, 8.1, 10 Technical Preview, Server 2008, 2008 R2, 2012, 2012 R2, Technical Preview.

Технология TrueCrypt является средством шифрования сторонних производителей с открытым исходным кодом, адаптированным под операционные системы семейства Windows, LINUX и MAC.

Для внедрения вышеупомянутых технологий шифрования информации на накопителе необходимо:

1. Произвести оценку готовности аппаратных ресурсов к технологиям BitLocker и TrueCrypt.

2. Произвести оценку программной среды для дальнейшего развертывания средств шифрования.

3. Выбрать наиболее подходящую под задачи конфигурацию BitLocker и TrueCrypt.

4. Создать план восстановления данных в случае непредвиденных обстоятельств.

Для того, чтобы можно было использовать BitLocker совместно с TrueCrypt, рабочие станции должны удовлетворять следующим требованиям:

1. При необходимости использования BitLocker вместе с модулем TPM, системные платы рабочих станций должны быть совместимы с TPM, то есть оборудованы чипами TPM соответствующими спецификации Trusted Computing Group TPM v.1.2 или выше.

2. Диск должен содержать два раздела с файловой системой NTFS. Раздел, на который BitLocker будет записывать загрузочные компоненты, должен быть активный и, в зависимости от версии операционной системы, содержать определенное количество свободного дискового пространства.

«Службы TPM обеспечивают сохранность данных, используя специализированный аппаратный компонент, называемый доверенным платформенным модулем (модуль TPM, Trusted Platform Module). Модуль TPM представляет собой микросхему, которая обычно встроена в системную плату компьютера и взаимодействует с системой по специальной шине» [6].

«Основное назначение микросхемы TPM в процессе надежного генерирования криптографических ключей – защита этих ключей и возможность работы в качестве аппаратного генератора псевдослучайных чисел» [7].

«В технологии BitLocker микросхема TPM используется для защиты ключей шифрования и обеспечения аутентификации путем проверки целостности надежного маршрута загрузки (то есть BIOS, загрузочного сектора и т.п.). Этот тип поддерживаемой TPM защиты выполняется только при работе BitLocker, либо в режиме прозрачного функционирования (Transparent Operation), либо в режиме аутентификации пользователя (User Authentication). В любом из этих режимов BitLocker использует микросхему TPM для выявления несанкционированных изменений загрузочной среды, такой как BIOS и главная загрузочная запись (MBR). При выявлении несанкционированных изменений BitLocker запросит предоставление ключей восстановления, прежде чем главный ключ тома (Volume Master Key) сможет быть расшифрован, и процесс загрузки компьютера сможет быть продолжен» [7].

Стоит отметить, что так как модуль TPM не зависит от операционной системы и имеет собственное программное обеспечение, то он фактически защищен от возможных уязвимостей операционной системы.

При оценке программной среды следует обратить внимание на операционные системы, под управлением которых будут функционировать два средства шифрования одновременно.

BitLocker поддерживает следующие операционные системы Microsoft:

1. Windows Vista редакции Максимальная и Корпоративная;
2. Windows 7 Максимальная и Корпоративная;
3. Windows 8.1 Профессиональная и Корпоративная;
4. Windows Server 2008;
5. Windows Server 2008 R2;
6. Windows Server 2012;
7. Windows Server 2012 R2.

При использовании других редакций или версий операционных систем Microsoft Windows возможна поддержка только программы TrueCrypt, так как они не поддерживают BitLocker.

При выборе конфигурации BitLocker и TrueCrypt необходимо определить наиболее подходящие под нее выдвигаемые задачи.

Доступны следующие режимы BitLocker:

1. BitLocker с TPM;
2. BitLocker с TPM и PIN-кодом;
3. BitLocker с TPM и USB устройством;
4. BitLocker с TPM и PIN-кодом и USB устройством;
5. BitLocker с USB устройством;
6. Пароль (режим доступен только под управлением OS MS Windows 8 и старше).

Варианты использования ТМП приведены в таблице 1.

Таблица 1
Table 1

Источник	Безопасность	Действия пользователя
TPM	Защищает от программных атак, но уязвим к аппаратным атакам	Никаких
TPM + PIN	Добавляет защиту от аппаратных атак	Пользователь должен вводить PIN-код при каждом запуске OS
TPM + ключ USB	Полная защита от аппаратных атак, но уязвима к потере ключа USB	Пользователь должен использовать ключ USB при каждом запуске OS
TPM + ключ USB + PIN	Максимальный уровень защиты	При каждом запуске OS пользователь должен вводить PIN-код и использовать ключ USB
Ключ USB	Минимальный уровень защиты для компьютеров, не оснащенных TPM + есть риск потери ключа	Пользователь должен использовать ключ USB при каждом запуске OS
Пароль	Минимальный уровень защиты	Пользователь должен использовать пароль при каждом запуске OS

Чтобы включить технологию BitLocker на диске с операционной системой без доверенного платформенного модуля (операционная система Microsoft Windows 7 Enterprise в виртуальной среде VMware Workstation 11) или воспользоваться другими функциями и параметрами BitLocker, необходимо изменить параметры групповой политики BitLocker, определяющие набор доступных функций в мастере установки BitLocker, а также иметь USB-устройство.

Вся требуемая информация ключа шифрования сохраняется на USB-устройстве. При запуске операционной системы необходимо вставить USB-устройство в компьютер. Ключ, хранящийся на USB-устройстве, позволяет разблокировать компьютер. Если на компьютере нет доверенного платформенного модуля, то вся требуемая для прочтения зашифрованного диска информация добавляется в ключ запуска.

Если для практической реализации использовать операционную систему Microsoft Windows 8.1, то можно воспользоваться только паролем, без использования USB-устройства.

Ключ запуска для компьютера без модуля TPM должен быть создан в течение инициализации шифрования BitLocker либо с помощью мастера настройки шифрования BitLocker, либо с помощью сценария. Шифрование BitLocker создает ключ запуска, пользователь вставляет флэш-диск USB, и система сохраняет ключ запуска на этом устройстве.

Когда система не оснащена модулем TPM (в среде виртуализации VMware данный модуль отсутствует), когда этот модуль отключен или когда в соответствии с настройками BIOS модуль TPM скрыт от операционной системы, мастер BitLocker Drive Encryption в фазе инициализации отображает сообщение об ошибке. Затем мастер предлагает пользователю выйти из процедуры установки BitLocker – нажатие кнопки Cancel является единственным вариантом продолжения, рекомендуемым системой.

Одна из настроек групповой политики операционной системы Microsoft Windows 7, равно как и в операционных системах Microsoft Windows Vista, 8, 8.1, Server 2008, 2008 R2, 2012, позволяет внести изменения в этот используемый по умолчанию режим работы. Чтобы изменить режим работы мастера BitLocker, необходимо запустить редактор групповых политик.

Для этого выбрать **Пуск → Выполнить →** ввести **gpedit.msc** и нажать **Enter**. Далее необходимо перейти в раздел **Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Шифрование диска BitLocker → Диски операционной системы**. Дважды щелкнуть на элементе **Обязательная дополнительная проверка подлинности при запуске**. Затем активировать радиокнопку **Включить**. После этого необходимо обновить редактор групповых политик, чтобы изменения вступили в силу.

После того, как изменения вступят в силу, мастер BitLocker не будет генерировать ошибку в связи с отсутствием или неверной настройкой модуля TPM.

После перезагрузки будет произведена настройка шифрования диска.

В качестве единственного предпочтительного варианта при запуске мастер укажет **Запрашивать ключ запуска при запуске**. Когда будет выбран этот предпочтительный вариант запуска, мастер предложит установить съемное запоминающее устройство USB для сохранения ключа запуска. После успешного завершения работы мастера BitLocker система будет всякий раз при загрузке предлагать устанавливать USB-ключ BitLocker.

К сожалению, BIOS VMware Workstation не поддерживает загрузку с USB (без дополнительных утилий), и реализовать данный метод защиты возможно лишь при ручном вводе при каждой загрузке операционной системы ключа восстановления BitLocker.

Следующим шагом защиты является шифрование уже зашифрованной операционной системы средствами TrueCrypt.

В главном меню программы TrueCrypt необходимо выбрать **Система → Зашифровать системный раздел/диск** и т.д. После зашифровки системного раздела во время загрузки операционной системы сначала необходимо будет вводить пароль от программы TrueCrypt, затем использовать USB накопитель для ввода ключа программы BitLocker.

Данная технология шифрования позволила применить использование различных средств шифрования одновременно. В указанном выше примере операционная система Microsoft Windows 7 Enterprise была зашифрована одновременно двумя различными средствами шифрования, а именно BitLocker и TrueCrypt. Таким методом выполняется защита рабочих станций в Академии ЛИМТУ Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. *Гаджиев Г.А.* Конституционные основы современного права собственности // Журнал российского права. – 2006. – № 12.
2. *Осовецкий Л.Г., Птицын А.В.* История и современная система защиты информации в России / Учеб. пособие. – СПб: СПб ГИТМО (ТУ), 2002. – 87 с.
3. *Голубев Е.А.* Стеганографические технологии – новое направление защиты информации. Журнал T-Comm – Телекоммуникации и Транспорт. – № 6. – 2012.
4. *Шлыков Г.Н.* Применение гомоморфизма в моделях защиты информации // Вестник Удмуртского университета. – № 2-4. – 2011.
5. *Котенко В.В.* Защита дискретной информации с позиций виртуализации информационных потоков // Известия Южного федерального университета. Технические науки. – № 4. – Том 129. – 2012.
6. *Станек У.Р.* Microsoft Windows 8. Справочник администратора. / У.Р. Станек. – Москва: Русская редакция; Санкт-Петербург: БХВ-Петербург, 2014. – 688 с.
7. *Моримото Р.* Microsoft Server 2012. Полное руководство / Р. Моримото, М. Нозл, Г. Ярдени, О. Драуби, Э. Аб-бейт, К. Амарис. – Москва: И.Д. Вильямс, 2013. – 1456 с.
8. www.truecrypt.org.
9. www.acronis.com.

REFERENCES

1. *Gadzhiev G.A.* Constitutional fundamentals of modern property rights [Constitutsionnye osnovy sovremennogo prava sobstvennosti]. *Zhurnal Rossiyskogo prava*. 2006, no. 12. Pp. 37-38. (in Russ.).
2. *Osoviecki L.G., Ptitsyn A.V.* History and modern system of data protection in Russia [Istoriya i sovremennaya sistema zashshity informatsii v Rossii]. *Uchebnoe posobie. Sankt-Peterburg, GITMO*, 2002. P. 87. (in Russ.).
3. *Golubev E.A.* Steganographic technology is a new area of information security [Steganograficheskie tekhnologii – novoe napravlenie zashshity informatsii]. *Jurnal T-Comm – telekommunikatsii i Transport*. No. 6, 2012. (in Russ.).
4. *Shlykov G.N.* The application of the homomorphism in models of information security [Primenenie gomomorfizma v modelyax zashshity informatsii]. *Journal Vestnik Udmurtskogo universiteta*. No. 2-4, 2011. (in Russ.).
5. *Kotenko V.V.* Protection of discrete information from the positions of the virtualization information flows [Zashshita diskretnoy informatsii s pozitsii virtualisatsii informatsionnykh potokov] *Journal Izvestiya Yuzhnogo federal'nogo universiteta. Tekhnicheskie nauki*. No. 4, tom 129, 2012. (in Russ.).
6. *Stanek U.R.* Microsoft Windows 8. Administrator's reference [Microsoft Windows 8 Spravochnik administratora]. *Sankt-Peterburg, BHV-Peterburg*, 2014. 688 p. (in Russ.).
7. *Morimoto R.* Microsoft Server 2012. The complete guide [Microsoft Server 2012. Polnoe rukovodstvo]. *Moskva: I.D. Williams*, 2013. 1456 p. (in Russ.).
8. Available at: www.truecrypt.org
9. Available at: www.acronis.com

Информация об авторе

Галашина Надежда Евгеньевна, преподаватель кафедры аппаратно-программных комплексов вычислительной техники Академии ЛИМТУ Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики.
beneke@yandex.ru

Костеж Владимир Александрович, кандидат технических наук, доцент кафедры аппаратно-программных комплексов вычислительной техники Академии ЛИМТУ Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики.
kostezh@mail.ru

Левковец Леонид Борисович, кандидат технических наук, доцент, профессор кафедры компьютерного проектирования и дизайна Академии ЛИМТУ Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики.
Санкт-Петербург, Россия
l_levkovets@mail.ru

Получена: 20.03.2015

Information about the author

Galashina Nadezhda Evgenyevna, Lecturer, the Chair of Software and Hardware of Computer Technologies, Academy LIMTU, St. Petersburg National Research University of Information Technologies, Mechanics and Optics.

beneke@yandex.ru

Kostezh Vladimir Alexandrovich, Candidate of Technical Sciences, Associate Professor, the Chair of Software and Hardware of Computer Technologies, Academy LIMTU, St. Petersburg National Research University of Information Technologies, Mechanics and Optics.

kostezh@mail.ru

Levkovets Leonid Borisovich, Candidate of Technical Sciences, Professor, Chair of Computer Design, Academy LIMTU, St. Petersburg National Research University of Information Technologies, Mechanics and Optics.

Sankt- Peterburg city, Russian Federation
l_levkovets@mail.ru

Received: 20.03.2015