# Шифрование в руках конечных пользователей

**Do you have something to say about this article?**
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

В рамках стратегии глубокой защиты многие организации наращивают применение шифрования. И хотя шифрование может защитить от несанкционированного доступа и уменьшить вероятность кражи данных, очень сложно внедрять системы и процессы, которые обеспечивали бы разумно необходимую уверенность в конфиденциальности при практическом применении. В последние годы многие продукты программного обеспечения начали предлагать встроенные функции шифрования более удобные в использовании и управлении. Если рассматривать специализированные средства шифрования обмена информацией или межсистемное стандартизированное шифрование, то у них, как правило, уже достаточно высокий уровень развития. Однако многие организации не готовы к рискам и проблемам, связанным с шифрованием, которым будут управлять конечные пользователи (межпользовательское шифрование).

## Призыв к шифрованию

Промышленный шпионаж, хакеры государственного масштаба и организованная преступность представляют собой проблему даже для самых маленьких организаций. Тем не менее, это не замедляет скорость сохранения и обмена данными между партнерами, регулирующими органами и клиентами. Сейчас организации совместно используют огромное количество собственных данных и личных данных сотрудников и клиентов на постоянной основе. Растущая осведомленность советов директоров и возрастающее давление со стороны регулирующих органов ведут к тому, что защите данных уделяется все больше внимания и финансирования.[1]

Большинство организаций сегодня без проблем внедряют транзитное шифрование. Отделы обеспечения безопасности с легкостью обосновывают необходимость в веб-приложениях, обеспечивающих безопасность на уровне транспортировки (протокол TLS), или же настаивают на выборе таких безопасных протоколов, как протокол передачи фалов (SFTP) и протокол безопасной командной оболочки (SSH). К сожалению, многие рабочие процессы передачи данных проходят вне контроля ИТ или должны соответствовать требованиям, установленным извне. В результате, критические данные и данные с высокой степенью риска по-прежнему отправляются по электронной почте и во вложениях. Все чаще и чаще пользователи также пользуются как санкционированными, так и несанкционированными облачными хранилищами и файлообменными службами. Из-за того, что все эти сценарии невозможно определить и проконтролировать, организации прибегают к внедрению инструментов шифрования для конечных пользователей в надежде на то, что пользователи будут достаточно ответственными и смогут интегрировать шифрование в существующие процессы (например, ИТ-отдел требует применять шифрование перед отправкой писем по электронной почте). Однако данный подход во многом делегирует ответственность за безопасность незаинтересованным конечным пользователям, которые ищут пути наименьшего сопротивления.[2]

## Добро пожаловать в джунгли

Теоретически, шифрование – это всего лишь применение некоторой математики к битам данных до и после отправки файла или сообщения. Тем не менее, существует огромная экосистема технологий, алгоритмов, конфигураций, инструментов и форматов шифрования. Еще более усложняют дело средства межпользовательского шифрования, которые славятся своим неудобством с точки зрения конечного пользователя.[3] Управление и передача ключей шифрования и/или паролей и обеспечение безопасного хранения – слишком сложные требования для конечных пользователей.

> **“Средства межпользовательского шифрования славятся своим неудобством с точки зрения конечного пользователя.”**

Даже при внедрении и обучении пользованию самыми лучшими и наиболее эффективно интегрированными средствами все равно остается проблема совместимости с партнерами. Если один из партнеров пользуется другой платформой, то развертывание такой платформы требует дополнительных инвестиций и усилий

**Эрик Голдман, CISA, Security+**
*Специалист по обеспечению безопасности информации с опытом работы в сфере финансовых услуг и промышленного производства. В области информационной безопасности специализируется на человеческом факторе и взаимодействиях человек-компьютер. С ним можно связаться по электронной почте Eric.Goldman@owasp.org.*

по внедрению. А если у организации много партнеров, то это стремительно повышает накладные расходы, связанные с приобретением и поддержкой нескольких программных средств. Если же не поддерживать работу средств, которые требуются конечным пользователям для удовлетворения требований своих бизнес-партнеров, то это приведет к тому, что конечные пользователи начнут искать творческие решения и способы обхода системы.

Помимо предоставления правильных «средств» необходимо также блокировать несанкционированные решения по шифрованию. Частично проблему решает «вайтлистинг» (белый список), однако, сегодняшний пользователь скорее будет искать решения в облаке и дело может кончится каким-нибудь ненадежным веб-сайтом. Проблема заключается в том, что пользование веб-сайтом не может отслеживаться или контролироваться. Кроме того, предоставляемые услуги могут быть незащищены надлежащим образом, а то и откровенно вредоносными. Например, такое средство может предлагать шифровать выгруженные файлы, но может неумышленно или специально сохранять незашифрованные оригиналы. Попытки пользователей повысить безопасность, к сожалению, могут привести к компрометированию данных.

Даже в списке утвержденных приложений могут быть средства, предоставляющие какой-либо вид шифрования в качестве дополнительной функции. Например, многие архиваторы позволяют пользоваться широко распространенной, но безумно устаревшей и слабой формой шифрования с файловым расширением .zip (см. примечание сбоку). Неразумно разрешать или поощрять пользование подобными средствами. Использование слабых или устаревших методов шифрования бесполезно с точки зрения безопасности, к тому же использование таких средств может отрицательно сказаться на репутации организации, поскольку партнеры могут воспринять это как некомпетентность или нежелание вкладывать средства в безопасность.

### Даже, если это работает...

Даже, если организация может внедрить средство, которое соответствует ее потребностям и совместимо со средствами партнеров, опасность все равно существует. Большинство средств не являются сквозными решениями, что повышает вероятность отрицательного влияния на процесс человеческого фактора. Некоторые средства могут быть разработаны не для предприятий и могут не позволять им отключать ненадлежащие параметры шифрования. Когда организация внедряет средства, она должна быть уверена, что команда, занимающаяся безопасностью, сможет отслеживать и контролировать алгоритмы, длину ключа и другие переменные. Например, если используются файлы Office Open XML (OOXML) (формат Microsoft Office 2007+), то можно централизованно контролировать длину пароля, сложность и алгоритмы с помощью центра развертывания Office/групповой политики.[4] Таким образом, при использовании файлов OOXML может обеспечить стандартизацию, однако, к сожалению, значения, заданные изначально, не являются безопасными по умолчанию. Нет никакой гарантии, что конфигурации организаций-партнеров будут адекватным образом соответствовать стандартам предприятия, а среды партнеров-аудиторов могут оказаться непрактичными. Помимо этого, предприятие не может быть уверено, что фильтры и другие средства не будут блокировать файлы по пути, поскольку вредоносная программа для Office является одной из самых известных угроз.

Даже если выполнено техническое внедрение и решены проблемы совместимости, следует также рассмотреть операционные процессы. Например, в случае с файлами OOXML, пользователь может сохранить зашифрованную копию в директории вместе с оригиналом и затем случайно вложить небезопасную версию (пользователи славятся своим неумением называть

## Пример с фалом Zip

Первая попытка, которую делают все организации при предоставлении средств шифрования, – это извлечь максимальную пользу из формата .zip. Большинство распространенных операционных систем поддерживают открытие защищенных паролем файлов с разрешением .zip, однако эта поддержка, как правило, ограничена вследствие устаревшей или слабой формы шифрования. Некоторые средства внешних разработчиков могут шифровать файлы .zip «крепким» шифрованием, однако это не гарантирует совместимости с системами получателя. Даже если оба партнера могут использовать более устойчивые конфигурации шифрования, нет уверенности в том, что пользователи выберут правильные параметры или придумают сильный пароль, поскольку многие архиваторы рассчитаны на одного пользователя и не позволяют административным образом обеспечивать возможные конфигурации.

файлы и при шифровании OOXML файла не меняют ни расширение файла, ни его значок (иконку). Умелые пользователи могут также обойти Политику группы, отправив оригинальный файл для работы дома и без ограничений пользоваться личной копией Office, что приводит к нежелательной, незашифрованной передаче данных во вне. В большинстве случаев, для шифрования, осуществляемого конечными пользователями, предпочтение отдается симметричному шифрованию на основе паролей, поскольку это позволяет избежать сложностей, связанных с управлением ключами/сертификатами. Однако, проблема обеспечения безопасного обмена данными заключается в том, что остается пароль. Возможно и можно внедрить средство или службу для такого обмена, но, опять же, существует проблема поддержки и совместимости. В результате, безопасное сообщение общего пароля по другому каналу доверяется пользователям (например, позвонить, чтобы сообщить пароль для вложения в электронной почте). Однако этим становится сложно управлять (какой пароль к какому сообщению), при этом пользователям будет трудно диктовать устно сложный, длинный или случайный пароль.

Основная цель шифрования – защитить файл даже, когда прямой доступ возможен или передача перехвачена, поэтому пользователи должны знать о риске недостаточного разделения зашифрованного содержимого и пароля. Ни в коем случае не следует просто отправлять пароль в другом письме. Службу коротких сообщений (SMS) также не следует рассматривать как отдельный канал, поскольку у многих пользователей программа электронной почты установлена на телефон, а вредоносные программы одинаково легко получают доступ как к электронной почте, так и к SMS-сообщениям. Вредоносные программы могут обнаружить зашифрованные сообщения, после чего сканировать все электронные письма, чтобы собрать словарь из уникальных слов или сочетаний фраз для тестирования в качестве потенциальных паролей. Атака может быть оптимизирована для поиска несловарных слов или ключевых фраз (например, «Пароль:...»).

### Неожиданные последствия

При внедрении шифрования, управляемого конечными пользователями, следует изучить его потенциальные отрицательные стороны. Для распознавания и предотвращения атак (например, антивирус, фильтры спама) и предотвращения кражи данных (DLP) необходимо проводить проверку содержимого. Обычно, средства анализа безопасности не обеспечивают централизованного управления или отслеживания криптоключей/паролей или других источников информации. Если систе-

## Шифрование не заменяет управление доступом

Как шифрование, так и управление доступом к системе обеспечивают конфиденциальность. Два ключевых различия состоят в том, что управление доступом позволяет со временем менять права доступа, а разрешение на доступ не имеет отношения к самим данным. Зашифрованный файл, по сути, включает в себя как проверку подлинности, так и разрешение доступа. Без дополнительной системы вы не сможете позднее, после того, как человек уже получил пароль или ключ, отозвать доступ. Невозможно получить назад цифровой файл. Кроме того, в отличие от управления доступом, вы не можете ограничить скорость передачи (например, отказывать в запросах, сделанных в пределах коротких временных промежутков) на случай попытки просто угадать пароль.

Шифрование иногда используют вместо управления доступом, но это ошибка. В таких случаях правильным решением является некоторый вариант управления цифровыми правами (УЦП) или управление информационными правами (УИП). В рамках УИП можно добавлять отправку на сервер команды о прекращении доступа даже, если предоставляется правильный пароль, что позволяет централизованно управлять доступом и за пределами организации.

Кроме того, в случае обмена файлами между организациями, шифрование само по себе не ограничивает повторное использование или дальнейший обмен, потому что получатель может спокойно дешифровать и удалить зашифрованный файл или поделиться с кем-то паролем дешифрования. Для строго конфиденциальной информации можно пользоваться безопасными виртуальными “комнатами данных».[5] В любом случае шифрование и УЦП не могут заменить другие методы управления использованием и обработкой такие, как юридические договора (например, соглашение о неразглашении информации) или установка видимых и водяных знаков. Само по себе предоставление зашифрованного документа, как правило юридически не обязывает другую сторону относится к этим данным каким бы то ни было особым образом.

ма предотвращения потери данных не может узнать пароль/ключ, она не может дешифровать и прочитать файл. Будет ли средство предотвращения потери данных блокировать отправку зашифрованного файла? Со стороны получателя вложения электронной почты не могут быть проверены на макровирусы, если фильтры электронной не могут дешифровать файл. В результате конечным пользователям приходится принимать больше сложных решений, всех последствий, которых они при этом не понимают.

Еще одним неожиданным последствием предоставления пользователям права заниматься шифрованием является риск отказа в обслуживании самого себя (DoS). Отказ в обслуживании, как правило, обсуждается в контексте серверов, однако файл, который нельзя дешифровать, является еще одной формой атаки типа «отказа в обслуживании» – представьте злоумышленников, пользующихся CryptoLocker и его вариантами.[6] Пользователь, который изо всех сил стремится к обеспечению безопасности, может шифровать все файлы. Это приведет к большому количеству паролей, которые надо будет помнить. Пользователь может использовать программу безопасного управления паролями, однако эти средства также, как правило, не оснащены функциями депонирования. Если такой пользователь уйдет из компании, больше ни у кого не будет доступа к этим зашифрованным документам.

Существуют также неочевидные последствия передачи конечным пользователям права на управление шифрованием. Например, как использование шифрования сочетается с требованиями к сохранению писем юридического характера или с другими аналогичными процессами архивирования? Как это повлияет на управление содержимым и осуществление поиска в данных? Шифрование также влияет на сжатие файлов, что может оказаться проблематичным для отправки вложений, учитывая ограничения по размеру. Когда на уровне файлов применяется много шифрования, следует продумать специальные процедуры резервного копирования и репликаций.

> **“Пользователям больше не нужно принимать решения о протоколах”**

### Преимущества централизации

Как правило, ИТ отделы либо пытаются найти функции шифрования в тех программных средствах, которые уже имеются, либо же внедряют одно или два специализированных пользовательский средства шифрования, которыми пользуются партнеры. Однако, в последние годы все доступнее становятся шлюзы/прокси-сервера шифрования. Подобно тому, как клиенты настольных приложений перешли к веб-приложениям, шлюз шифрования позволяет централизовать процесс шифрования и усилить контроль и управление со стороны ИТ-отдела. Как и в случае любого другого прокси-сервера, данные перемещаются по шине, и шифрование/дешифрование может применяться прозрачно и автоматически.

Централизованное развертывание позволяет намного легче устанавливать связи с другими партнерами, пользующимися централизованными решениями даже от разных поставщиков. Обмен ключами и сертификатами можно оставить специалистам, а для передачи можно использовать стандартизованные протоколы. Пользователям больше не нужно принимать решения о протоколах, что позволяет ИТ-отделам вместе разрабатывать приемлемые конфигурации или же прибегать к межкомпьютерным согласованиям, чтобы разрешались только согласованные параметры шифрования. Даже если получатель пользуется другой платформой, все равно можно грамотно присоединить пользователя/организацию, по максимуму использовать возможности платформы УЦП или привлечь безопасный файлообменный ресурс (по крайней мере, управление файлами).

Можно уменьшить нагрузку на пользователей, нажав на кнопку или вставив ключевое слово (например, «Зашифровать») в строку темы электронного письма. Для подготовки файла или депонирования ключа/пароля организации также могут развернуть веб-портал или средство «перетаскивания» файлов. Средства предотвращения потери данных или почтовые фильтры способны грамотно определять необходимость шифрования, когда пользователь забывает об этом, или же могут перенаправлять пользователей и блокировать передачу.[7] Для получателя файл может быть дешифрован автоматически централизованно или же сохранен до получения разрешения от пользователя, таким образом, между дешифрованием и получением конечным пользователем доступа к файлу проходят этапы «проверка» и «песочница».

### Ограничение на санкционированное шифрование

После развертывания централизованного или управляемого пользователем решения, необходимо принять меры для бло-

## Кто является владельцем данных?

Шифрование обычно применяется с целью обезопасить обмен данными между двумя или более индивидами и, соответственно, владельцами данных являются только участники обмена. Однако, если речь идет о коммерческой деятельности, то здесь владельцами данных скорее являются организации, а не отдельные пользователи. Многие протоколы шифрования сообщений и отдельные средства шифрования файлов изначально разрабатываются для личного пользования. Тем не менее, в корпоративной среде зачастую необходимо обладать некоторым вариантом депонирования ключей или функцией просмотра незашифрованных версий данных теми, кто напрямую не участвует в транзакции, например, юридический отдел или отдел обеспечения безопасности (или по крайней мере, применяемые ими автоматизированные средства).

Когда кто-то оценивает программное обеспечение или системы шифрования, важно учитывать, как эти средства повлияют на законный доступ организации к данным. Если средства предусмотрены для организаций, они тем или иным образом интегрируются в систему предотвращения потери данных или в систему обнаружения вторжений, например, открытый текст, передача ключей или согласование перед шифрованием с локальными агентами программы. Такие системы также должны безопасным образом управлять всеми ключами/паролями, чтобы предупредить неправильное использование или вероятное воздействие со стороны хакеров, а также в соответствующих случаях включать рабочие процессы утверждения и ведения журналов.

Личная переписка может и должна полагаться на комплексные, не допускающие обходов технологии шифрования для предотвращения прослушивания/ перехвата. На предприятиях главная проблема собственности данных состоит в том, что пользователи должны понимать и соглашаться с тем, что обмен информацией происходит не между людьми, а между организациями.

кирования несанкционированного шифрования и «ухода» зашифрованных файлов по несанкционированным каналам. Это помогает заблокировать устаревшие алгоритмы шифрования и не позволяет внутренним злоумышленникам или хакерам использовать шифрование для эксфильтрации данных. Такого рода проверка и блокировка уже распространены в безопасных Интернет-транзакциях.[8] Правила системы предотвращения потери данных следует задавать для блокировки любого шифрования, которое не может быть проверено и/или идет по неутвержденной службе, порту или назначению.
Помимо этого, рекомендуется отслеживать программное обеспечение и процессы в пользовательских системах, чтобы гарантировать, что никто не установил и не пользуется несанкционированными программами шифрования. При обнаружении подобного программного обеспечения, следует провести расследование и определить, существует ли обоснованная потребность в этом рабочем процессе и можно ли его преобразовать под другое, санкционированное средство шифрования. В связи с растущим использованием облачных технологий, следует проверять Интернет-трафик для блокирования несанкционированных веб-сайтов и служб, которыми пользовались или могут попытаться пользоваться пользователи для шифрования или дешифрования данных.

### Заручитесь пониманием и осведомленностью пользователей

Даже при прозрачных решениях крайне важно проводить надлежащее обучение пользователей для того, чтобы они понимали свои возможности и обязанности в связи с шифрованием. Пользователи должны понимать, что шифрование – это не просто защита паролем и что не все типы шифрования одинаковы.
Системы предотвращения утечки данных (DLP) и искусственного интеллекта (AI) никогда не смогут «отловить» все случаи, требующие шифрования, поэтому лучше всего обучать пользователей тому, как вручную запустить процесс шифрования, это позволит им спокойно относиться к этому вопросу. Также следует регулярно проводить повышение квалификации или переподготовку.
Для большей ясности рекомендуется определить и сформулировать политику в отношении шифрования. Предприятие должно четко определить утвержденные средства конфигурации, процедуры и последовательность действий так, чтобы у пользователей не возникало неопределенности.

> **“шифрование – это не просто защита паролем и что не все типы шифрования одинаковы”**

Например, пользователи не должны отправлять зашифрованные данные домой (например, при отсутствии персональных средств зашифрованного резервного копирования). В политике информационной безопасности должно быть четко указано, что руководство оставляет за собой право, в разрешенных законодательством случаях, проверять и дешифровывать любой обмен информацией и файлы из соображений безопасности, в соответствии с законом или в других соответствующих случаях.

## Заключение

Организации должны знать о проблемах и рисках, связанных с передачей шифрования в руки пользователей. Помимо нахождения и настройки правильной технологии, предприятия должны следить за тем, чтобы процессы были хорошо определены, а пользователи в достаточной степени обучены. Централизованное решение, с одной стороны, позволит сократить затраты и силы, направленные на поддержку, а с другой – повысит эффективность интеграции с системами предотвращения утечки данных (DLP). В любом случае шифрование должно быть контролируемым и ограниченным, в противном случае в области обеспечения безопасности у вас образуется мертвая зона.

## Примечания


1 NYSE Governance Services and Veracode, A 2015 Survey: Cybersecurity In The Boardroom («Исследование 2015 года: Кибербезопасность в зале заседаний совета директоров»), 2015 год, https://www.nyse.com/publicdocs/VERACODE_Survey_Report.pdf

2 Besnard, D.; B. Arief; "Computer Security Impaired by Legitimate Users," («Негативное влияние законных пользователей на компьютерную безопасность») Computers & Security, vol. 23, iss. 3, 2004 год, стр. 253-264

3 Whitten, A.; J. D. Tygar; "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," («Почему Джонни не может шифровать: оценка практичности PGP 5.0») USENIX Security Symposium, 1999 год, стр. 169-184, https://www.usenix.org/legacy/events/sec99/ full_papers/whitten/whitten_html/

4 Microsoft Technet, "Group Policy and Office Customization Tool Settings in Office 2010 for OpenDocument and Office Open XML Formats" («Групповая политика и параметры центра развертывания Office в Office 2010 для форматов OpenDocument и Office Open XML»), 2016 год, https://technet.microsoft.com/pt-br/library/

5 Pang, A.; D. Stanton; T. Nagle; "Managing Cyber- Security Risks in M&A" («Управление рисками кибербезопасности при слияниях и поглощениях»), Financier Worldwide, июль 2014 года, www.financierworldwide.com/managingcyber- security-risks-in-ma

6 ФБР США, "Criminals Continue to Defraud and Extort Funds From Victims Using Cryptowall Ransomware Schemes" («Преступники продолжают обманным путем выманивать средства у жертв, пользуясь схемами программы Cryptowall Ransomware» Internet Crime Complaint Center (IC3), 23 июня 2015 года, www.ic3.gov/media/2015/150623.aspx

7 Microsoft, "Conditions and Exceptions for Transport Rules" («Условия и исключения для правил транспортировки»), Microsoft Developer Network, 2010 год, https://msdn.microsoft.com/en-us/library/ ff628740(v=exchsrvcs.149).aspx#Attachments

8 Lyngaas, S.; "Decrypting Outbound Data: A Key to Security," *FCW*, 11 August 2015, *https://fcw.com/articles/2015/08/11/ssl-encryption.aspx*