ПЕРВЫЙ МЕТР – главная линия защиты конфиденциальной информации

И.Тимофеев, к.э.н., ООО "Фирма "АНКАД"

В статье приводятся сведения о наиболее актуальных угрозах безопасности конфиденциальной информации, современных требованиях к средствам защиты и существующих способах решения. Автор предлагает новый подход к защите конфиденциальной информации, оптимальный по соотношению цена/уровень защиты.

Эпоха информационного общества вместе с огромными возможностями несет в себе и большие угрозы. Информационные потоки окружают нас повсюду – доступ к информации упростился, в том числе и к той ее части, которая должна быть скрыта от посторонних глаз. Это касается не только государственной тайны и коммерческой информации, но и персональных данных, а также личной информации.

Конфиденциальная информация (КИ) может находиться в трех состояниях – хранение, обработка и передача. Необходимость надежной защиты информации при передаче не вызывает сомнений, и человечество занимается этим с древних времен. Но, как ни странно, задачи защиты информации при передаче по открытым сетям в целом решены. При использовании шифрования передаваемой информации надежным алгоритмом и сохранении ключа в тайне вскрытие информации при перехвате в открытых сетях практически невозможно. Существует множество способов организации такой передачи: возможно шифрование отдельных файлов, сообщений электронной почты, создание зашифрованных VPN-сетей и т.п. При хранении информации шифрование используется так же широко и успешно.

Но при обработке конфиденциальной информации – создании, редактировании, ознакомлении – требуется ее визуализация, и в этот момент она не может быть зашифрована, а чтобы получить доступ к информации для ее обработки, необходимо ввести в систему пароль и предоставить ей доступ к ключу. К тому же надежность криптографической защиты зависит не только от алгоритма шифрования и сохранения в тайне секретных ключей, но и от надежной защиты самого процесса шифрования. Таким образом, большинство актуальных угроз информационной безопасности сосредоточены в настоящий момент на рабочих местах пользователей: рабочем или домашнем компьютере или устройстве мобильного доступа – планшете, смартфоне, так называемом "первом метре", на котором происходит обработка информации (рис.1).

Решение, обеспечивающее приемлемый уровень защищенности КИ во всех трех возможных состояниях (обработки, хранения, и передачи), прежде всего, в границах "первого метра", могло бы стать достойным ответом

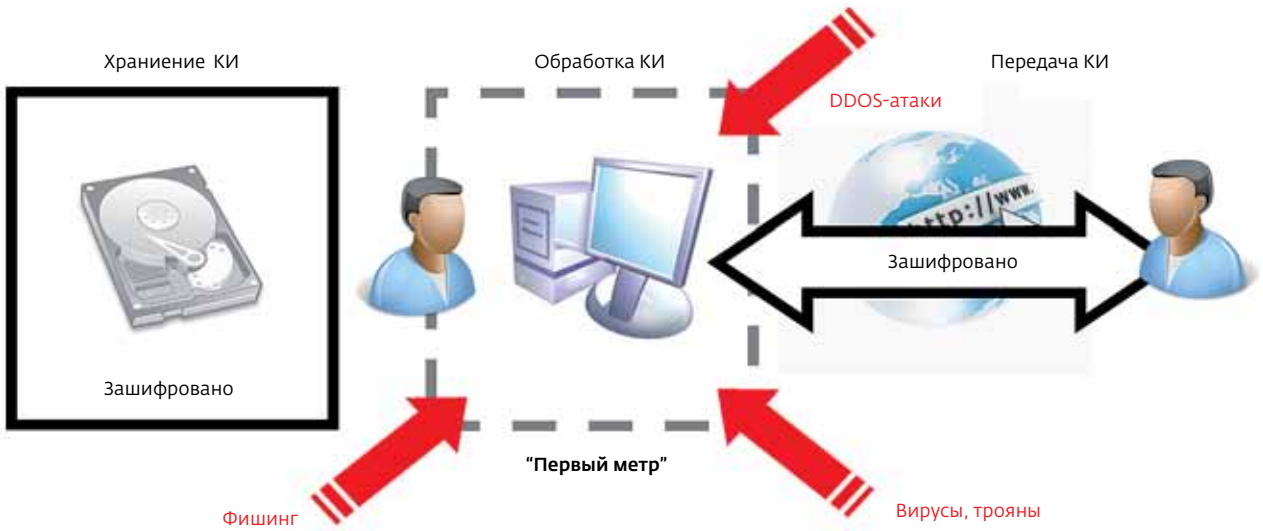

Рис.1. "Первый метр" защиты конфиденциальной информации

на современные вызовы информационной безопасности (ИБ).

Внутри периметра "первого метра" у злоумышленника существует ряд возможностей для получения доступа к паролям, ключам шифрования и непосредственно КИ:

- уязвимость ИБ наиболее популярных операционных систем (ОС);
- недокументированные возможности (закладки) программного обеспечения (ПО), которыми могут воспользоваться как злоумышленники, так и недобросовестные производители ПО;
- использование личных устройств на рабочем месте (распространение так называемой концепции BYOD – bring your own device – "принеси свое собственное устройство").

Для реализации этих возможностей применяются различные технологии похищения пароля ("фишинг"), компьютерные вирусы и "трояны", осуществляется целевой взлом корпоративных и персональных информационных систем. Также большой проблемой при доступе к корпоративным ресурсам через общедоступные сети становятся атаки типа "отказ в обслуживании" (DDOS-атаки), которые блокируют доступ легальных пользователей к конфиденциальной информации.

Конечно, существует множество средств защиты и от этих угроз: антивирусные программы, межсетевые экраны, модули доверенной загрузки, системы контроля и разграничения доступа (в том числе клиент-серверные системы), системы защиты от утечек (DLP-системы) и др. Применение этих средств в комплексе является довольно затратным как по финансам, так и по организационным ресурсам, и зачастую под силу только крупным компаниям, в то время как 100%-ной гарантии информационной безопасности эти средства все равно не дают. Малым предприятиям и индивидуальным пользователям приходиться довольствоваться средствами попроще, а значит, менее надежными, закрывающими не все виды угроз.

Помимо защиты от актуальных угроз средство защиты должно соответствовать требованиям современных пользователей, которые они предъявляют к любым информационным системам, а именно:

- универсальность: возможность использования с разными типами компьютеров;
- мобильность;
- гибкость: различные исполнения, настраиваемые параметры;
- низкая цена;
- отсутствие ограничений на обычную работу: использование привычного программного обеспечения, выход в Интернет и др.

Массовый рынок предлагает сейчас различные средства ИБ, направленные на удовлетворение запросов широкого круга пользователей, которые, как и любые средства широкого применения, имеют свои недостатки:

Рис.2. "Анкадер" на защите "первого метра"

- чисто программные решения, в том числе и бесплатные. Они подвержены множеству программных атак;
- программные решения с использованием аппаратного ключа – токена. Токен позволяет достаточно надежно защитить ключ, но не защищает КИ в процессе ее обработки;
- защищенные USB-носители (флешки) либо устройства "флешка и токен в одном корпусе". При обработке информации она все равно попадает в незащищенную операционную систему.

Помимо необходимости использования аутентификации, шифрования КИ и использования защищенных ключевых носителей, все больше экспертов в области информационной безопасности склоняются к тому, что обязательным требованием при работе с конфиденциальной информацией является наличие доверенной операционной среды.

Под доверенной операционной средой здесь подразумевается операционная система (и ПО) со встроенными средствами защиты, в которой отсутствуют недекларированные возможности и обеспечивается ее целостность (неизменность).

В настоящее время на рынке существуют несколько типов систем с доверенной средой:

- комплексные системы с аппаратными модулями доверенной загрузки, системами разграничения доступа и аппаратными шифраторами. Они достаточно сложные в использовании и обслуживании, имеют высокую стоимость и ограниченную мобильность;
- системы создания доверенного сеанса работы. Существует необходимость подключения к корпоративному серверу, кроме того, у них высокая стоимость;
- системы с доверенной операционной средой, загружаемой в одно ядро многоядерного центрального процессора компьютера. Результат – очень маленькие ресурсы для операционной системы и, как следствие, – ее очень ограниченная функциональность: невозможно работать с различными форматами файлов и др.

Итак, современному пользователю, заинтересованному в защите своей конфиденциальной информации, требуется мобильное, универсальное, но в то же время надежное средство для хранения и обработки конфиденциальной информации с обязательным наличием аппаратного компонента защиты, доверенной операционной среды для обработки, а также с использованием криптографических методов защиты. Кроме того, оно должно быть простым в использовании и доступным по цене.

Наша компания предлагает новый подход и новое компактное устройство, которое как удовлетворяет постоянно возрастающим потребностям широкого круга пользователей, так и соответствует современным требованиям ИБ в условиях актуальных угроз "первого метра" (рис.2).

Средство защиты конфиденциальной информации (СЗКИ) "Анкадер" (Ancuder) представляет собой устройство, реализованное в форм-факторе небольшого USB-носителя и объединяющее в себе три компонента:

- носитель информации общим объемом памяти от 8 Гб, имеющий открытую и защищенную (зашифрованную) области памяти;
- доверенную операционную систему на базе Linux со встроенными средствами защиты (идентификация и аутентификация, шифрование алгоритмом ГОСТ 28147-89, контроль целостности, протоколирование) и ПО Libre Office;
- защищенный ключевой носитель на базе отечественного сертифицированного криптопроцессора.

СЗКИ "Анкадер" предназначено для защиты КИ во всех трех ее состояниях. Хранение информации осуществляется в зашифрованром виде, ключ шифрования хранится в защищенной памяти криптопроцессора и никогда его не покидает. Доступ к ключу возможен только при знании пароля. Обработка информации осуществляется только в доверенной среде, загружаемой на компьютер пользователя. Доступ к информации для обработки открывается только после успешной аутентификации. Передача конфиденциальной информации в открытом виде запрещена.

Новый подход, реализованный при разработке этого решения, обеспечивает его преимущества по сравнению с другими предлагаемыми рынком средствами ИБ:

- возможность совмещения на одном устройстве хранения как рабочей конфиденциальной информации, так и личной информации сотрудников без дополнительных угроз безопасности для тех и других;
- возможность использования одного устройства для переноса как открытой, так и конфиденциальной информации без ущерба защищенности последней;
- возможность использования на различных компьютерах (сейчас архитектуры x86, в перспективе – архитектуры ARM), независимость от ОС, установленной на конкретном компьютере, и ее уязвимости.

Технологии защиты, реализованные в устройстве, позволяют использовать его в различных случаях, когда требуется защита информации:

- защита личной информации частного лица, хранение паролей пользователя для доступа к различным ресурсам;
- защита персональных данных (в соответствии со ст. 152 ФЗ);
- защита коммерческой тайны как крупных, так и малых предприятий и индивидуальных предпринимателей;
- квалифицированная электронная цифровая подпись (ЭЦП) электронных документов;
- аутентификация при доступе к web-ресурсам, в том числе к Порталу госуслуг.

Зачастую многие пользователи вовсе отказываются от использования средств защиты информации или ограничиваются самой простой парольной защитой, предоставляемой ОС или прикладным ПО. Мотивируется это тем, что стоимость высокозащищенных систем намного выше, чем вероятный ущерб от угроз ИБ, и их использование связано с рядом неудобств, а простые системы в случае реальной опасности серьезной защиты не дают. Но в настоящий момент на рынке представлены средства с различным соотношением цены, удобства и уровня защиты, и пользователи могут выбрать подходящие им, исходя из собственной оценки рисков информационной безопасности и имеющихся ресурсов. Уровень осознания необходимости информационной безопасности растет, и каждый человек может идти в ногу со временем, используя имеющиеся возможности. ■