



## Двухфакторная аутентификация RSA SecurID

**RSA SecurID** - мощное решение в области двухфакторной аутентификации. В любой, даже самой защищенной системе обеспечения информационной безопасности - слабым звеном был и остается пользователь. Парольная политика - вечный источник головной боли администраторов безопасности, ведь каждое из решений таит свои подводные камни. Предоставив пользователям полную свободу в выборе пароля, рискуешь оказаться в ситуации, когда 80% пользователей используют пароль «123456», а оставшиеся 20% - пароль «qwerty». Если парольная политика запрещает использование слабых паролей – пользователи решают эту проблему просто – пишут пароли на стикерах и клеят на монитор, те, кто заботятся о безопасности – прячут под клавиатуру. Кроме того, в крупных компаниях, десятки человеко-часов сотрудников технической поддержки уходят на восстановление паролей забывчивых пользователей. Компания RSA предлагает решение позволяющее снизить расходы на поддержку пользователей, упростить вашим сотрудникам жизнь и значительно повысить безопасность данных.

Двухфакторная аутентификация означает, что подтверждение легитимности пользователя происходит в два этапа: сначала пользователь предьявляет нечто, что он знает (пароль, PIN), затем нечто, что он имеет (токен, смарткарту). Повышение уровня защищенности при использовании двухфакторной аутентификации очевидно. Разнообразные методы хищения паролей, кейлогеры, социальная инженерия и прочее - перестают действовать. Вместо перехвата пароля злоумышленнику необходимо будет узнать PIN, похитить token и воспользоваться этими атрибутами доступа, в тот краткий промежуток времени, пока пользователь не обнаружил пропажу и не обратился в техподдержку с просьбой заблокировать утерянный token.

Кроме того, RSA позволяет значительно сэкономить на времени работников службы ТП, затраченных на восстановление паролей пользователей, времени беспомощности самих пользователей и киловаттах ментальных усилий необходимых пользователям на запоминание сложных комбинаций букв и цифр.

Используя технологию SecurID Вы не только значительно повысите уровень защищенности корпоративных данных, но и порядком сэкономите на обработке запросов в техподдержку от пользователей забывших пароль.

### Использование решения для финансовых структур.

RSA опубликовала результаты четвертого ежегодного опроса клиентов финансовых учреждений об онлайн мошенничествах. В ходе проведенного Интернет-опроса было собрано мнение 1 678 человек (взрослых, имеющих не менее одного банковского счета) из восьми стран мира по вопросам, связанным с развитием фишинга, «вишинга» и использования программ регистрации нажатий клавиши, а также с усилиями финансовых учреждений по укреплению методов авторизации банковских операций по удаленному каналу. Основные результаты опроса таковы: 91% владельцев счетов ответили, что они хотели бы перейти от стандартного метода авторизации, использующего имя пользователя и пароль, к новому методу аутентификации в случае принятия их банками более эффективных мер безопасности. 73% опрошенных хотели бы, чтобы их финансовые организации использовали аутентификацию, основанную на риске. Такая идентификация проводится на основе таких факторов, как место регистрации, IP-адрес и поведение при транзакции, к которым могут добавляться телефонные звонки на частотах вне основного диапазона частот и секретные вопросы для транзакций, считающихся очень рискованными. 40% опрошенных в различных странах мира ответили, что в качестве метода идентификации хотели бы использовать «токены». Активными сторонниками этой технологии были владельцы счетов в Испании, Германии, Сингапуре и Индии. Причем 46-50% респондентов ответили, что они хотели бы использовать аппаратные ключи. При этом 49% сказали, что, если допустить, что их банк принял решение использовать в качестве метода онлайн-идентификация «токенов», было бы хорошо, если бы эти же ключи можно было бы использовать при регистрации не только на сайте с сервисом online banking, но и на других веб-сайтах. 56% респондентов ответили, что они хотели бы использовать персонализированное изображение для аутентификации пользователя при его регистрации на сайте online banking, 53% считают, что персонализированное изображение позволяет им чувствовать себя более защищенными от атак хакеров. Пользователи выбирают персонализированное изображение и используют его для того, чтобы убедиться, что они действительно находятся на законном сайте банка, а не на подставном. 69% владельцев счетов считают, что финансовые учреждения должны заменить регистрацию на основе имени пользователя и пароля более

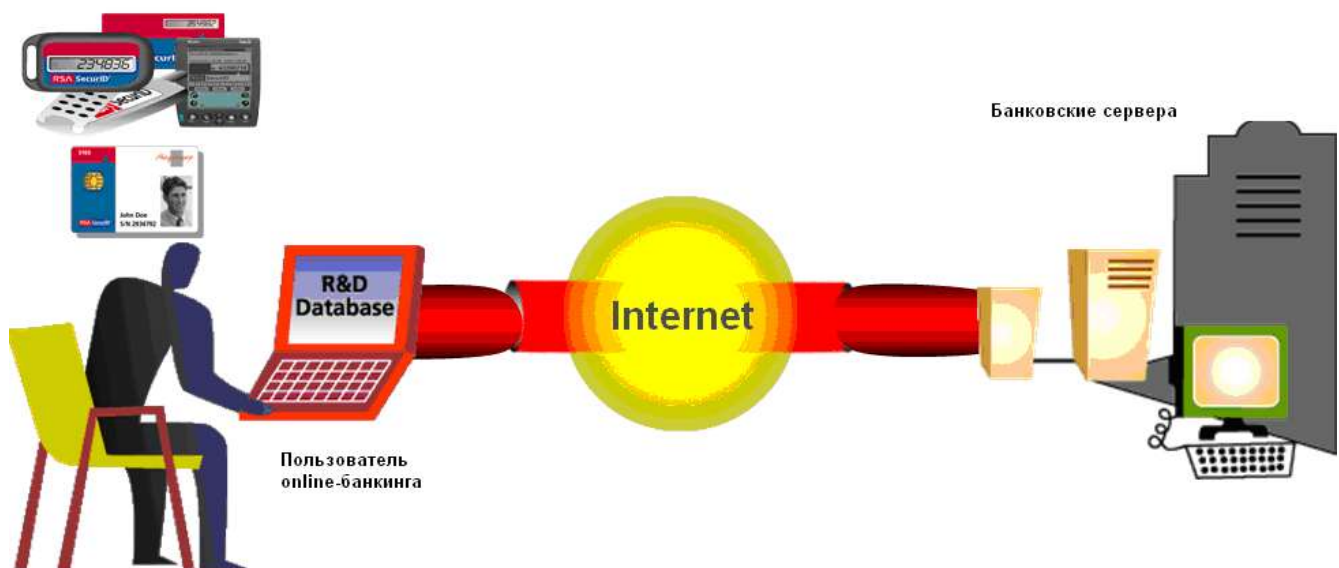
эффективным методом аутентификации для систем *online banking*. 58% владельцев счетов считают, что финансовые учреждения должны развернуть более эффективные методы аутентификации для систем оказания банковских услуг через телефонную линию (*telephone banking*). 82% владельцев банковских счетов хотели бы, чтобы их банки отслеживали признаки незаконных видов деятельности в сеансах связи с системами *online banking* и *telephone banking* аналогично тому, как это сегодня делается при контроле кредитных карточек. 51% считают, что при обнаружении подозрительных онлайн-банковских операций банки должны сообщать им об этом, а 48% полагают, что аналогичное следует делать для сервиса *telephone banking*. Британские владельцы счетов особенно озабочены этой проблемой: 93% опрошенных в Великобритании заявили, что они хотели бы, чтобы их онлайн-банковские операции контролировались. Во Франции об этом заявили 70% респондентов. Многие финансовые организации начали переход к развертыванию более эффективных методов аутентификации только в прошлом году, о них знают лишь 39% владельцев счетов. Менее 70% респондентов в Великобритании (69%) и Австралии (65%) заявили, что знакомы с термином «фишинг». В США это число составляет 83% опрошенных. Кроме того, доверие к операциям, выполняемым через Интернет, продолжает падать. 82% владельцев счетов заявили, что вряд ли они ответят на электронную почту, связанную с банковским обслуживанием, из-за различных видов мошенничества, включая фишинг. Это число увеличилось по сравнению с показателями в 79% опрошенных в предыдущие годы. Более половины всех респондентов заявили, что, скорее всего, они не подписались бы на сервис *online banking*. Кроме того, 44% владельцев счетов заявили, что за последние шесть месяцев значительно выросла их обеспокоенность, связанная с другими типами угроз (кроме фишинга), например, с вирусами и программой отслеживания и сохранения нажатий клавиш

Как и в любых других организациях, двухфакторную аутентификацию можно использовать для защиты критичных учетных записей, таких как аккаунты топ-менеджеров или IT-администраторов. Однако, эта технология в банковской сфере находит еще одно применение – повышение защиты пользователей услуги *internet-банкинга*.

Вместо управляющего программного обеспечения, т.н. **RSA Authentication Manager**, банковская структура может приобрести специальные библиотеки от компании RSA, реализующие аналогичный функционал. Это значительно дешевле и появляется возможность встроить этот функционал в собственное программное обеспечение.

Помимо обычных токенов, дающих возможность использовать одноразовые пароли, можно использовать специальные токены, обладающие возможностью подписи финансовых транзакций, для категории VIP, реализующих крупные финансовые переводы. В случае использования токенов RSA для *e-банкинга*, компания-вендор готова предоставить значительные, весьма значительные скидки под крупные закупки.

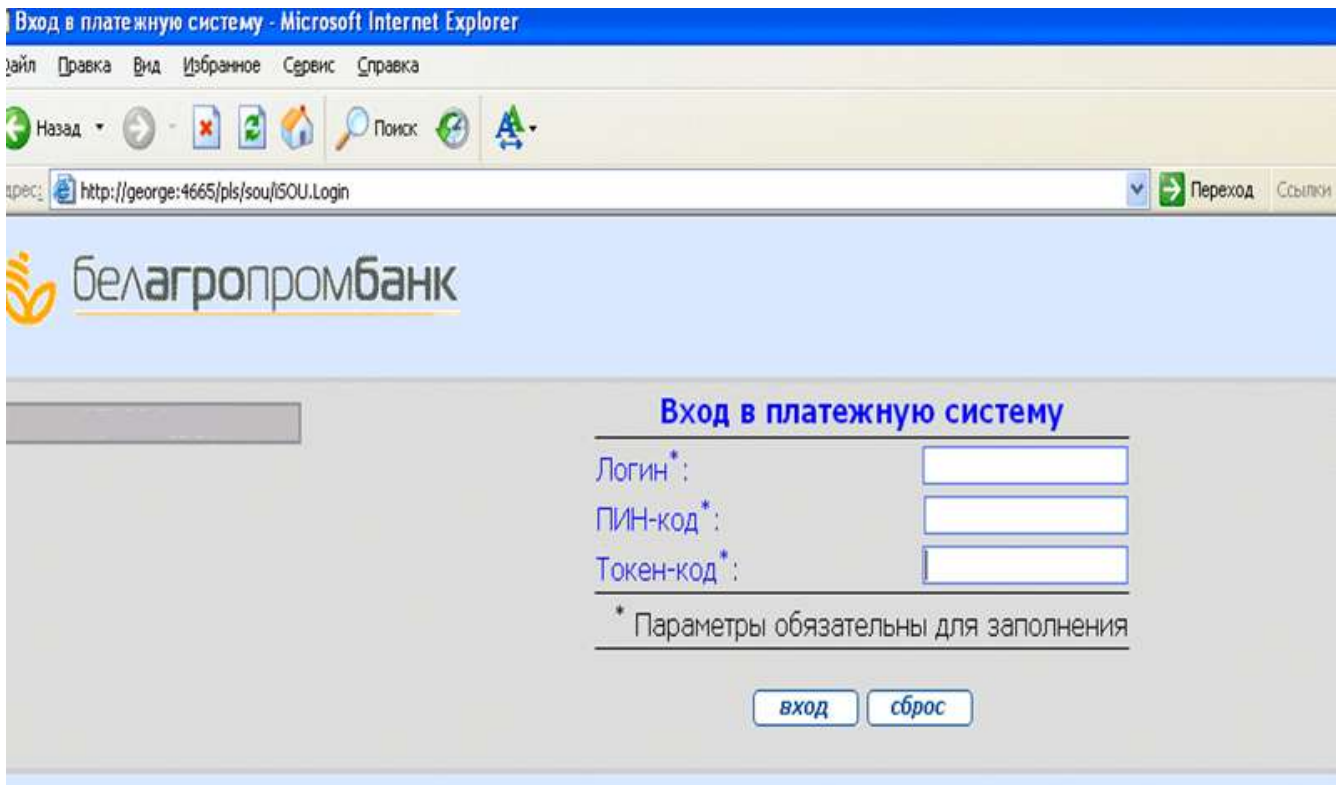
Схема работы *internet-банкинга*



Обычный токен RSA, функционал OTP, SID700



Токен с возможностью подписи финансовых транзакций, SID900



Пример системы internet-банкинга в действии

Прочие примеры и бизнес-кейсы

*Бизнес-кейс I. Решение RSA SecurID было использовано финансовой компанией Vajaj Capital.*

*Vajaj Capital Group – одна из наиболее крупных консалтинговых компаний занимающихся инвестициями и финансовым планированием. В 2008 году, Vajaj Capital открыли web-портал для брокерских и инвестиционных операций, однако возникла проблема безопасной авторизации, ведь завладев паролем пользователя, злоумышленники получали доступ к огромным суммам. В качестве решения, компания установила у себя Authentication Manager и предложила своим заказчикам аппаратные токены SecurID. Благодаря этому решению, компания заметно повысила уверенность своих клиентов в защищенности их активов, вследствие чего Vajaj Capital планирует привлечь более 300 000 новых клиентов в течении ближайших трех лет.*

*Бизнес-кейс II. Решение RSA SecurID - Asia United Bank (AUB). В процессе расширения спектра сервисных услуг Asia United Bank (AUB) создали web-портал, с помощью которого клиенты могли управлять своим банковским аккаунтом. Для того, чтобы избежать угрозы мошенничества и хищений, руководство банка приняло решение снабдить своих клиентов токенами двухфакторной аутентификации RSA SecurID. Это позволило клиентам получить безопасный доступ к к порталу из любой точки мира. В результате банк получил легко масштабируемое и безопасное решение, которое позволило значительно повысить уровень доверия пользователей к системе управление аккаунтом, что сильно сказалось на их лояльность к банку в целом.*



*Бизнес-кейс III. Techcombank – крупный вьетнамский банк, использующий самые передовые технологии. В процессе расширения деятельности, руководство банка решило предоставить пользователям новую услугу. Те, кто хотел лучше защитить свои активы, мог приобрести дополнительную услугу двухфакторной аутентификации, на основе решения RSA SecurID. Важным критерием выбора была возможность предоставить пользователю уверенность в эффективности защиты. Это стало возможным, благодаря использованию бренда RSA, известному во всем мире более 15 лет. В июле 2007-го года из более чем 100 000 клиентов банка, 20% использовали двухфакторную аутентификацию. В течении 2008 года это число возросло в 4 раза. В результате использования двухфакторной аутентификации от RSA Techcombank не только получил прибыль от продажи дополнительной услуги, а и значительно укрепил свои позиции и репутацию банка использующего самые передовые технологии и защищающего деньги своих клиентов.*