Эпоха биометрии: как защитить персональные данные

А. САБАНОВ: «ПРИ ВЫБОРЕ ИНСТРУМЕНТА ЗАЩИТЫ СЛЕДУЕТ ИСХОДИТЬ НЕ ТОЛЬКО ИЗ ОЦЕНКИ ЕГО ДОСТУПНОСТИ ИЛИ НЕДОСТУПНОСТИ ПО ЦЕНОВОМУ ПАРАМЕТРУ, А ИЗ ТОГО, КАКУЮ ЦЕНУ ОПЕРАТОР МОЖЕТ ЗАПЛАТИТЬ В СЛУЧАЕ РЕАЛИЗАЦИИ РИСКОВ»

Беседовала: Елена Елисеенкова

Защита персональных данных – это та тема, которая сейчас в контексте ужесточения регулирования в сфере ИБ наиболее актуальна для банковских организаций. Какие ИБ-системы оптимально использовать для решения этой задачи? Чем объясняется то, что банки пока еще предпочитают организационные меры шифрованию данных? На эти и другие вопросы ответил в интервью NBJ заместитель генерального директора компании «Аладдин Р.Д.» Алексей САБАНОВ.

NBJ: Алексей, первый вопрос, который хотелось бы вам задать, следующий. Как вы оцениваете ситуацию с защитой персональных данных (ПДн) клиентов и иной конфиденциальной информации в финансовом секторе?

А. САБАНОВ: Казалось бы, здесь все очень просто. Есть 152-ФЗ, в соответствии с которым персональные данные подлежат защите, а оператор ПДн несет ответственность за разглашение этих сведений без согласия субъекта персональных данных или его представителя, за невыполнение требований об уточнении, блокировке, уничтожении данных, а также в ряде других случаев. Но так гладко все выглядит только на бумаге...

NBJ: А на самом деле?

А. САБАНОВ: А на самом деле банки и другие финансовые организации по-разному решают эти задачи, а некоторые этого вообще не делают. Речь идет о малых финансово-кредитных организациях, у которых нет средств для содержания специалистов по защите информации. В лучшем случае такие банки привлекают аутсорсеров для решения подобных задач, в худшем вообще игнорируют это, надеясь, что ничего страшного не произойдет. Они также могут формировать и согласовывать такие модели угроз и нарушителей, которые маскируют реальные угрозы безопасности.

NBJ: Но таких банков наверняка меньшинство, не так ли?

А. САБАНОВ: Их немного, но все же они есть. Конечно, в крупных банках дело обстоит иначе. У них есть целый штат сотрудников, которые отвечают за выполнение требований регулятора в части работы с персональными данными, за соответствие деятельности банка в этой сфере российскому законодательству. Но при этом подходы различаются. В некоторых банках господствует точка зрения, что для обеспечения защиты персональных данных и конфиденциальной информации достаточно исключительно организационных мер. Есть другое мнение – что данные ни в коем случае нельзя шифровать, потому что есть риск потери ключа, с помощью которого проводилось шифрование, и они могут пропасть.

NBJ: Разве такие прецеденты бывали?

А. САБАНОВ: Крайне редко, но тем не менее такой риск действительно

существует. Другое дело, что он реализуется не в силу независящих от банка обстоятельств, а потому, что не выполняются инструкции по предписанным регламентам шифрования. Но давайте от этих частных случаев перейдем к общей картине и сравним российский и западный подходы к защите персональных данных на примере международной организации ISO, экспертом которой я являюсь. Соответствующая рабочая группа сформулировала целый пул задач по идентификации, аутентификации, управлению доступом и шифрованию информации, по применению биометрии в части обеспечения защиты конфиденциальных данных. Понятно, что далеко не все из них на сегодняшний день решены, и очевидно, что здесь, безусловно, должна быть связь и с рисками, и с ИТ-архитектурой. Эти задачи актуальны и для наших банков, а, что еще необходимо отметить, и западные, и наши стандарты в сфере ИБ меняются в последние годы в одном и том же направлении.

NBJ: В каком именно?

А. САБАНОВ: Все большего «закручивания гаек», то есть ужесточения требований, когда речь идет о сборе, использовании, хранении и защите ПДн. С 25 мая текущего года в странах ЕС стали работать новые требования GDPR (General Data Protection Regulation, общий регламент по защите данных. – *Прим. ред.*), и при их изучении становится очевидным, что требования к ответственности операторов ПДн серьезно выросли.

NBJ: Наши банки обязаны соблюдать положения GDPR?

А. САБАНОВ: Они должны соблюдать российское законодательство, и де факто они не выполняют требования GDPR. Мало кто обращает внимание на тот факт, что клиенты могут обращаться в Международный суд по правам человека с исками о нарушении операторами их прав при обработке, использовании и хранении ПДн. Пока таких прецедентов нет, но это не означает, что их не будет в дальнейшем.

NBJ: И все же в чем главные различия в нашей и международной практике защиты ПДн?

А. САБАНОВ: У нас строго регулируется сам процесс защиты персональных данных, и если вы, как банк, строго классифицировали свою систему по определенному классу защищенности, то вам не надо думать, какие средства защиты информации использовать, поскольку вам их «подскажут» методические указания ФСТЭК и ФСБ России. У европейцев иной подход. Там все построено на оценке рисков, и оператор сам делает это и может самостоятельно выбирать средства защиты информации.

NBJ: На что банкам необходимо смотреть в первую очередь, когда речь идет о защите ПДн, и почему, по вашему мнению, сама по себе эта тема приобрела в последнее время такую актуальность?

А. САБАНОВ: В первую очередь банки должны следовать стандарту СТО БР ИББС и приказам Банка России, поскольку в таких случаях отраслевые стандарты принципиально важны. И тут я должен отметить, что эти предписания и указания достаточно понятны и прозрачны для финансово-кредитных организаций, но, к сожалению, не все банки выполняют их.

NBJ: Это странно, если учесть, что регулятор не просто рекомендует своим поднадзорным субъектам совершать те или иные действия по защите ПДн, а требует проведения внутреннего и внешнего аудита систем защиты ПДн и даже говорит о том, что недалек тот день, когда киберриски начнут учитываться при расчете капиталов банков и при формировании резервов.

А. САБАНОВ: Все это верно, но давайте не забывать о том, что на практике защита ПДн – очень сложная задача для банковских организаций, в том числе и для тех, которые занимают у нас ведущие позиции. Причина проста: у крупных банков за годы их деятельности накопилось большое количество информационных баз, в которых содержатся ПДн юридических и физических лиц. Это система клиент-банк, интернет-банкинг, кредитные досье юридических и физических лиц и т.д. Какую из этих баз и в какой степени надо защищать – именно эту задачу банкам и приходится решать. И трудно было бы ожидать при таком разнообразии баз и накопленного объема информации другого решения данного вопроса.

Это один момент. Второй – в большинстве банков до сих пор используются преимущественно импортные системы управления базами данных (СУБД). Импортное производство подразумевает наличие недекларируемых возможностей в системном ПО. Обойтись тут только организационными мерами и встроенными системами защиты не получится. Это упрощенный подход, который не даст желаемого результата. Но следует признать, что именно его придерживается, по моим наблюдениям, большинство банков.

NBJ: Какие риски у банков возникают в связи с этим?

> Я ДОЛЖЕН ОТМЕТИТЬ, ЧТО СТАНДАРТ СТО БР ИББС, ПРИКАЗЫ, ПРЕДПИСАНИЯ И УКАЗАНИЯ БАНКА РОССИИ ДОСТАТОЧНО ПОНЯТНЫ И ПРОЗРАЧНЫ ДЛЯ ФИНАНСОВО-КРЕДИТНЫХ ОРГАНИЗАЦИЙ, НО, К СОЖАЛЕНИЮ, НЕ ВСЕ БАНКИ ВЫПОЛНЯЮТ ИХ

В НЕКОТОРЫХ БАНКАХ ГОСПОДСТВУЕТ ТОЧКА ЗРЕНИЯ, ЧТО ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ДОСТАТОЧНО ИСКЛЮЧИТЕЛЬНО ОРГАНИЗАЦИОННЫХ МЕР

А. САБАНОВ: Во-первых, возможен сговор между сотрудником банка и неким лицом или лицами «на стороне». Сотрудник банка, имеющий права администратора системы, может изменить персональные данные или частично уничтожить их, а замести после этого следы ему не составит особого труда. Есть средства, которые могут исключить этот риск, например, КРИПТО БД – система предотвращения утечек информации из основных промышленных СУБД. Она построена таким образом, что привилегированные пользователи, в частности администраторы, видят данные только в зашифрованном виде. Конечно, можно попробовать подобрать ключ шифрования, но на это уйдут многие годы. К тому же в системе отражается, кто и когда вносил или пытался внести изменения в персональные данные, и, что принципиально важно, аудит системы производится наложенными средствами, то есть извне. Соответственно, повлиять на его результаты сотрудники банка не могут.

NBJ: КРИПТО БД – известный на рынке продукт, который используется многими организациями уже не первый год. За время, прошедшее с его запуска, он существенно изменился?

А. САБАНОВ: Безусловно, он менялся. Продукт был выпущен 12 лет назад, при этом сам по себе этот проект был начат 15 лет назад. С чем связано это различие в сроках? С тем, что прежде чем создавать наложенные средства защиты, почти три года велось углубленное изучение встроенных в СУБД методов защиты. И вы понимаете, что тогда, то есть 15 лет назад, были совершенно иными и законодательство по защите персональных данных, и регулирование киберрисков, и объемы персональных данных, которыми оперировали банки, и действия злоумышленников. Нам приходится все это учитывать, тем более что мы убеждены в том, что у КРИПТО БД очень хорошие перспективы в будущем, поскольку на сегодняшний день эта система шифрования в СУБД является единственной сертифицированной по требованиям ФСБ к средствам криптографической защиты информации (СКЗИ).

NBJ: То есть в этом вопросе ваша компания фактически является первопроходцем?

А. САБАНОВ: Да. Мы надеемся, что со временем появятся конкурентные решения, поскольку конкуренция, бесспорно, способствует дальнейшему развитию продуктов и проектов. Но пока мы видим, что предлагаемые решения других производителей имеют несколько иную направленность и в любом случае не поднимаются по качеству защиты и системности до уровня КРИПТО БД.

NBJ: Во многих ли банках работает эта система?

А. САБАНОВ: Вы, наверное, не поверите, но как раз в банках ее до сих пор ни разу не внедряли. У нас есть реализованные и очень успешные проекты по ее внедрению и использованию в самых различных отраслях – связи, здравоохранении, в юридической и пенсионной. А вот в банках нет, и, как мне представляется, они очень многое теряют, по тем или иным причинам отказываясь от внедрения КРИПТО БД, тем более что пилотный проект является бесплатным. Иными словами, у банков есть возможность, не неся дополнительных финансовых расходов, «обкатать» эту систему на практике, посмотреть, как она работает и какую минимизацию рисков она обеспечивает в сфере обработки и хранения ПДн.

NBJ: Вы наверняка как-то объясняете сами себе это нежелание.

А. САБАНОВ: Честно говоря, для меня это непонятно. Есть банки, которые объясняют свое нежелание внедрять КРИПТО БД опасением, что работа с зашифрованными данными приведет к фатальной потере производительности имеющихся у банков информационных систем. Но этот аргумент не выдерживает критики: если и есть потери в производительности систем, то они, как правило, наблюдаются очень недолго и исчисляются небольшими процентами, а то и долями процента. Это связано с тем, что КРИПТО БД позволяет защитить информацию адресно, из многих терабайтов данных будут зашифрованы только те, без которых остальная часть не имеет ценности. Мне представляется, что по крайней мере сейчас более важную роль в поведении банков играет дань моде.

NBJ: Что вы имеете в виду?

А. САБАНОВ: Очевидно, что все увлеклись биометрической идентификацией и склонны рассматривать ее как панацею от всех бед и защиту от всех угроз. Хотя на самом деле это не так, использовать биометрические данные небезопасно, а применяться они могут только как подтверждение владения традиционными идентификаторами с определенным (не таким высоким, как бы хотелось) порогом вероятности. Но в этом адептам биометрии еще только предстоит убедиться на собственном опыте. Что же касается шифрования, то здесь уже накоплен определенный опыт применения этого инструмента, и он наглядно демонстрирует, что шифрование данных действительно повышает общий уровень защищенности операторов и субъектов ПДн, тем более что предлагаемое нами решение дополнено функциями современного управления доступом к чувствительным данным.

ОЧЕВИДНО, ЧТО ВСЕ УВЛЕКЛИСЬ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИЕЙ И СКЛОННЫ РАССМАТРИВАТЬ ЕЕ КАК ПАНАЦЕЮ ОТ ВСЕХ БЕД И ЗАЩИТУ ОТ ВСЕХ УГРОЗ, ХОТЯ НА САМОМ ДЕЛЕ ЭТО НЕ ТАК

NBJ: И тем не менее биометрия вызывает сейчас больший интерес.

А. САБАНОВ: Тут, скорее всего, «включается», с одной стороны, стремление к чему-то новому, к инструменту, который объявляется сейчас наиболее прогрессивным. А с другой стороны, срабатывают необоснованные страхи – а вдруг будут утеряны ключи шифрования, и, соответственно, станут недоступными данные, которые были зашифрованы с помощью этих ключей, и т.д. Я думаю, что достаточно будет появиться одному смелому банку, который сумеет преодолеть эти страхи, и тогда настроения в банковском секторе, а также отношение участников рынка к системе КРИПТО БД изменятся. Рано или поздно это произойдет, но, по-видимому, банковской сфере еще предстоит «дозреть» до этого. К тому же всем тем, кто собирает биометрические данные, стоит задуматься и об их сохранности, т.е. целостности и конфиденциальности. Кроме того, насколько я знаю текущую ситуацию, пока не решен вопрос о том, кто и как будет отвечать за их утечки: банк, который их собирает, оператор Единой биометрической системы или тот, кто защищает каналы передачи. Вопросов здесь больше, чем ответов. Опыт других стран показывает, что сложностей при управлении цифровыми идентификационными данными в национальном масштабе очень много и они увеличиваются по мере роста накопленных баз. Поэтому в мире уровень охвата населения подобными проектами невысок, во всяком случае не выявлено ни одной страны со стопроцентным охватом населения.

NBJ: Возможно, определенным «стоп-фактором» для банков является цена вашего продукта? Не секрет, что ведущие представители банковской сферы предпочитают разрабатывать собственные решения, в том числе и в ИБ. Насколько доступно по ценовым параметрам решение КРИПТО БД для тех, кто относится к числу малых и средних кредитных организаций?

А. САБАНОВ: Оно вполне доступно и им. К тому же, когда мы говорим о доступности или недоступности того или иного решения по ценовому параметру, надо иметь в виду не только финансовые возможности потенциального покупателя, но и то, какую цену он может заплатить при реализации рисков. В данном случае речь, конечно же, идет о опасности потери и/или компрометации персональных данных клиентов. Как я уже говорил, и наше, и международное законодательство и регулирование в этом вопросе ужесточаются.

NBJ: И скупой может заплатить дважды?

А. САБАНОВ: Да. Но в любом случае наша ценовая политика выстраивается таким образом, что мы можем предложить банкам со сравнительно небольшим количеством обслуживаемых физических и юридических лиц приемлемые для них условия внедрения с помощью наших многочисленных партнеров. Кроме того, есть еще один момент, который, как мне кажется, будет подталкивать банки, независимо от их размеров, к внедрению КРИПТО БД. Вступает в действие 189-ФЗ о критической информационной инфраструктуре, и в этом контексте наличие средств защиты такого класса и уровня, как КРИПТО БД, становится для банков, как операторов персональных данных, не прихотью, а необходимостью. Мы, со своей стороны, также готовимся к этому: у нас проводится целая кампания по улучшению качества наших продуктов и повышению уровня ответственности за них. Поэтому я считаю, что перспективы здесь очень хорошие, и я приглашаю те банки, которые хотят попробовать КРИПТО БД для решения своих задач, сделать это как можно скорее. NBJ