



Оценка соответствия ОАО «Банк ВТБ Северо-Запад» требованиям стандарта СТО БР ИББС-1.0

Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации (СТО БР ИББС) – комплекс документов Банка России, описывающий единый подход к построению системы обеспечения ИБ организаций банковской сферы с учётом требований российского законодательства.



Федеральным Законом от 27.12.2002 № 184-ФЗ «О техническом регулировании» установлен рекомендательный статус стандартов и иных документов по стандартизации. Однако в соответствии с указанным Федеральным Законом стандарты и иные документы по стандартизации подлежат обязательному исполнению в организациях, если они добровольно принимают решение о присоединении.

ЗАДАЧА

В марте 2011 года ОАО «Банк ВТБ Северо-Запад» был реорганизован – присоединен к Банку ВТБ и на его базе был создан Северо-Западный региональный центр Банка ВТБ. В процессе подготовки присоединения стало очевидно, что необходим специальный инструмент регуляции внутренних процессов обеспечения информационной безопасности (ИБ), оценки лояльности сотрудников и рисков, связанных с утечкой данных – организованная система ИБ. К моменту интеграции банковских структур у ВТБ Северо-Запад уже была система ИБ, однако она требовала модернизации.

При создании или модернизации системы ИБ принято ориентироваться на уже имеющийся опыт и лучшие практики в отрасли. Для отечественных кредитно-финансовых организаций отражением таких практик является стандарт СТО БР ИББС-1.0, разработанный Банком России. Стандарт описывает основные требования к системе ИБ с учетом особенностей российского банковского бизнеса и законодательства. Кроме того, стандарт определяет требования к системе менеджмента ИБ – как и на каких уровнях должны взаимодействовать люди, технологии и процессы в банке для эффективного управления ИБ.

Несмотря на то, что стандарт СТО БР ИББС-1.0 носит рекомендательный характер, ему стремятся соответствовать многие организации банковской сферы, так как он затрагивает широкий спектр механизмов обеспечения информационной безопасности. Кроме того, СТО БР ИББС-1.0 был разработан на основе широко известных международных стандартов и включает в себя лучшие мировые практики по обеспечению ИБ. Поэтому за основу новой системы ИБ в Банке ВТБ Северо-Запад было решено принять положения именно этого стандарта.

По итогам тендера на проведение оценки соответствия стандарту СТО БР ИББС-1.0, для реализации проекта была приглашена компания «Инфосистемы Джет», которая имеет богатый практический опыт в области оказания консалтинговых услуг по обеспечению ИБ для организаций кредитно-финансовой отрасли. Также немаловажную роль в принятии решения сыграл тот факт, что интегратор уже несколько лет является членом ABISS (Association for Banking Information Security Standards)*. До недавнего времени в состав ABISS входили только банки и компании, обеспечивающие деятельность финансового сектора. Компания «Инфосистемы Джет» – один из первых партнеров ABISS в России среди ИТ-компаний.

РЕШЕНИЕ

В первую очередь специалисты компании «Инфосистемы Джет» провели комплексное обследование текущего уровня обеспечения ИБ. Это позволило понять, какие именно процессы и средства информационной безопасности не соответствуют требованиям стандарта, а также опре-

* ABISS – открытое сообщество, созданное как инструмент для развития и продвижения стандартов, положений и методических указаний Банка России, регулирующих деятельность служб ИБ банковской системы Российской Федерации.





127015 Россия, г. Москва,
ул. Б. Новодмитровская, д. 14, стр.1
Телефон: +7 (495) 411-7601
Факс: +7 (495) 411-7602
info@jet.msk.su
www.jet.msk.su



Серов Андрей Юрьевич,
руководитель Дирекции по
обеспечению безопасности

«В процессе оценки соответствия, консультанты не только давали четкие рекомендации нашим сотрудникам, но также отвечали на многие вопросы, выходящие за рамки проекта. Тем самым они проявили себя как специалисты широкого профиля в области информационной безопасности. Для нас аудит на соответствие СТО БР ИББС-1.0 – это важный шаг на пути развития бизнеса, возможность отладить внутренние механизмы компании, сделать ее еще более надежной для наших партнеров и клиентов».

делить необходимые меры для повышения уровня ИБ. Информация для анализа была собрана из самых разных источников: использовались материалы бесед с сотрудниками службы безопасности банка, внутренние регламентирующие документы, служебные записки, данные, полученные от специалистов банка по ИБ.

По результатам обследования был составлен подробный отчет о выявленных несоответствиях и представлены детальные рекомендации по их устранению. В процессе обсуждения замечаний, специалисты компании «Инфосистемы Джет» учитывали комментарии и пожелания ключевых сотрудников банка: руководства банка и начальников ИТ-служб.

*«Обычно мы получаем много комментариев со стороны специалистов, чья область деятельности подвергается оценке, – поясняет **Алексей Гришин, менеджер проекта компании «Инфосистемы Джет».** – Это логично, сотрудники компании всегда лучше знают устройство внутренних бизнес-процессов и могут объяснить, с чем связаны те или иные отклонения. В силу различных факторов невозможно построить идеальную систему ИБ, но можно сделать ее адекватной, работоспособной и эффективной. Без двустороннего взаимодействия нам сложно предложить оптимальное решение, а нашим коллегам на стороне заказчика – осознать и принять доводы консультантов. Сотрудники Банка ВТБ Северо-Запад изначально были настроены на конструктивную совместную работу. Это позволило нам оперативно согласовать результаты оценки и успешно завершить проект».*

В дополнение к рекомендациям по устранению выявленных несоответствий требованиям стандарта, специалисты компании «Инфосистемы Джет» подготовили предложения по модернизации системы менеджмента ИБ банка.

РЕЗУЛЬТАТ

Результатом проекта для банка стала инициация процесса приведения ИТ-инфраструктуры банка в соответствие со стандартом Банка России СТО БР ИББС-1.0. Банк ВТБ Северо-Запад получил квалифицированную оценку текущего уровня обеспечения информационной безопасности, а также набор практических рекомендаций по выполнению требований стандарта, которые касались не только вопросов обеспечения ИБ, но и модернизации ИТ-инфраструктуры в целом.

Аудит завершился в рекордно короткие сроки. Стандартно на проекты подобного рода отводится порядка 3 месяцев. В данном случае консультанты справились чуть более, чем за 2.

*«Проект Банка ВТБ Северо-Запад стал очень важным этапом в развитии наших компетенций по стандарту СТО БР ИББС-1.0, – резюмирует **Даниил Чернов, руководитель направления экспертных услуг по ИБ компании «Инфосистемы Джет».** – На нем мы отработали некоторые изменения в методологии ведения подобных проектов и наилучшим образом продемонстрировали свои компетенции не только в области оценки соответствия стандарту, но и в разработке конкретных практических рекомендаций по повышению уровня ИБ банка».*

