Система управления информационной безопасностью в банках Украины – время собирать камни

Наиболее значимым событием 2011 года в сфере банковской безопасности стало введение систем управления информационной безопасностью (СУИБ) в банках Украины. Истек предельный срок, отведенный Национальным банком Украины для их внедрения. О предварительных итогах этого масштабного мероприятия «Банкиру» рассказывает Директор Департамента информационных технологий НБУ Алексей БИЛАШ.

Алексей Алексеевич, насколько наши банки оказались готовыми к внедрению предложенной НБУ системы?

– Еще в июне 2010 года банки были проинформированы о необходимости внедрения СУИБ, а также о разрабатываемом стандарте НБУ в этой области. 28.10.2010 г. Национальный банк принял Постановление № 474 «О введении в действие стандартов по управлению информационной безопасностью в банковской системе Украины», которым обязал банки Украины до 01.10.2011 г. их внедрить в соответствии со стандартами НБУ. Текст стандартов СОУ Н НБУ 65.1 СУИБ 1.0:2010 «Методы защиты в банковской деятельности. Система управления информационной безопасностью. Требования» (ISO / IES 27001:2005, MOD) и СОУ Н НБУ 65.1 СУИБ 2.0:2010 «Методы защиты в банковской деятельности. Свод правил для управления информационной безопасностью» (ISO/IES 27002:2005, MOD) банки получили вместе с постановлением. 1 марта 2011 года НБУ утвердил и направил банкам соответствующие методические рекомендации.

Следовательно, у банков было достаточно времени, чтобы начать работы по внедрению СУИБ, имея всю необходимую информацию от регулятора. Что касается результатов, то условно все банки можно разделить на две категории. Первая – это банки, которые ответственно и сознательно подошли к инициативе НБУ в области контроля и снижения информационных рисков в рамках операционных рисков банков и, как следствие, укрепления всей банковской системы Украины. Они начали процесс по внедрению СУИБ с создания соответствующего комитета и рассмотрения возможности выполнения проекта собственными силами или с привлечением стороннего консультанта, а затем реализация перешла в практическую плоскость. Сейчас такие банки находятся на разных стадиях внедрения СУИБ и уже получили первые позитивные результаты.

Вторая – банки, которые ожидали и ждут практики применения санкций НБУ к банкам, нарушающим требования регулятора. Их логика сводится к вопросу, что дешевле – внедрить СУИБ или оплачивать штрафные санкции. Я считаю, что им надо задуматься над таким подходом, так как практика внедрения любых международных, внутригосударственных и отраслевых стандартов в мире сводится не к цели не платить какие-либо штрафы, а к тому, чтобы действительно уменьшать риски и увеличивать стабильность и прибыльность бизнеса. Именно это было основной целью Национального банка Украины при разработке и введении в действие отраслевых стандартов по СУИБ.

Существует ли взаимосвязь между размером капитала банков и эффективностью внедрения СУИБ?

– Размеры банков не оказывают прямого влияния на принятие решения и скорость внедрения СУИБ. В настоящее время Нацбанк имеет информацию о запущенных проектах по СУИБ в банках всех четырех групп. Двумя факторами, которые действительно влияют на этот процесс, можно назвать уровень зрелости банка (бизнеса банка с точки зрения применения лучших международных практик), а также выделение бюджета на проект внедрения СУИБ. Конечно, многие банки могут мотивировать свое бездействие по внедрению СУИБ отсутствием денег

вследствие влияния мирового экономического кризиса и снижения ликвидности банковских учреждений, а также нежеланием акционеров выделять ресурсы на проекты, которые ошибочно рас сматриваются как неприбыльные или затратные. Но если объективно оценивать, то надо понимать, что применение СУИБ позволяет банкам не нести потери, связанные с рисками угроз и уязвимо сти информсистем, а также опти мизировать затраты по обеспечению информационной безопасности и автоматизации бизнеса (инвестиции в IT-технологии). Ведь при оценке рисков можно оценить потенциальные потери и, как результат, рационально подойти к вложениям, направленным на предотвращение таких рисков и угроз.

Банки с иностранным капиталом действительно имеют в своем распоряжении ряд наработок по внедрению СУИБ, так как их материнские структуры стремятся к соответствию требованиям между народных стандартов, в том числе и серии стандартов ISO / IES 2700x. При этом есть значительное число банков с украинским капиталом, которые грамотно подходят к внутренней нормативной документации и управлению процессами и имеют достаточный для внедрения СУИБ уровень зрелости.

Б С 1 октября 2011 года начались проверки Национальным банком Украины СУИБ банков. С какими наиболее характерными проблемами столкнулись банки в процессе внедрения?

– Уже на первом этапе внедрения СУИБ основной проблемой является отсутствие понимания бизнес-подразделениями целей и задач внедрения системы управления, а также зачастую СУИБ рассматривается не как система менеджмента а как средство обеспечения защиты информации – программно-аппаратный комплекс. Для того чтобы донести корректное понимание сути СУИБ, НБУ был проведен ряд учебных мероприятий для сотрудников банков. Существенной проблемой при внедрении СУИБ стало отсутствие, устаревшее или неактуальное/некорректное описание критических бизнес-процессов, которые должны быть оценены в рамках реализации проекта. Кроме того, возникает целый ряд вопросов по определению владельцев бизнес-процессов, и, как следствие, все это вносит задержки при внедрении СУИБ. Эффективное решение – привлечение профессиональных компаний-консультантов, которые обладают значительным опытом в области построения систем менеджмента, систем информационной безопасности и описания бизнес-процессов.

Б Внедрение украинскими банками СУИБ на уровне стандартов НБУ позволит им соответствовать международным стандартам ISO 27001 и ISO 27002 и получить подтверждающие это сертификаты. Сколько банков сегодня готово провести их сертификацию, и как изменилось это число за последний год?

– Есть ошибочное мнение, что при прохождении банком сертификации на соответствие стандартам серии ISO 27000 автоматически реализуются требования СУИБ НБУ. Данный миф появился вследствие того, что внутриотраслевой стандарт НБУ разработан на их базе. При внедрении и соответствии требованиям стандартов СОУ Н НБУ 65.1 СУИБ банк уже на 100% готов к прохождению аудита международным органом по сертификации на соответствие требованиям ISO 27001, но не наоборот. Стандарт НБУ ужесточен всеми существующими требованиями Национального банка Украины в области защиты информации. Например, такими как «Правила организации защиты электронных банковских документов с использованием средств защиты информации», «Правила технической защиты помещений банков, в которых обрабатываются электронные банковские документы», «Правила хранения, защиты, использования и раскрытия банковской тайны», «Положение об обеспечении непрерывного функционирования информационных систем», «Положение о порядке формирования, хранения и уничтожения электронных архивов» и другими нормативно-правовыми актами регулятора. Кроме того, в СУИБ НБУ не допускаются исключения требований, которые могут быть применены банком при внедрении ISO 27001. Также серьезным отличием стандарта СОУ Н НБУ 65.1 СУИБ от стандартов ISO 27001 и ISO 27002 является подход к оценке рисков: в рамках СУИБ НБУ оцениваются риски бизнес-процессов, а в рамках ISO 27001 – применяются к конкретному ресурсу. То есть стандарт НБУ намного шире и эффективнее для применения к специфике банковской деятельности.

Б Планирует ли НБУ стимулировать получение банками соответствующих сертификатов, или это останется на усмотрении банков?

– Регулятор проверяет выполнение банками своих требований в рамках проверок подразделениями банковского надзора Национального банка Украины. Получение сертификатов соответствия международным стандартам не регламентируется и является персональным решением каждого отдельного банка.

Б Как украинские банки предпочитают решать вопросы, связанные с внедрением СУИБ – собственными силами или через аутсорсинг?

– Часть банков реализует проекты собственными внутренними ресурсами. Но чаще, насколько нам известно, они привлекают для этого сторонних консультантов. Кроме того, внедрением СУИБ заинтересовались и небанковские финансовые организации.

Б Каковы планы Департамента информационных технологий НБУ на будущий год в области внедрения, совершенствования и контроля СУИБ?

– Мы планируем продолжить работу в области информации о необходимости внедрения СУИБ, а также проведение цикла учебных мероприятий, которые помогут банкам разобраться в ее тонкостях. Также Национальный Банк ведет проект внедрения СУИБ для внутренних целей. Департамент информационных технологий, а также Управление защиты информации НБУ тесно сотрудничают с подразделениями банковского надзора, что позволит максимально эффективно проводить проверки банков на соответствие требованиям Регулятора. Так как первичной целью внедрения СУИБ Национальный банк изначально ставил укрепление всей банковской системы Украины, я уверен, что украинские банки активно включатся в процесс ее внедрения и получат от этого явные преимущества.

Подготовил Сергей ЛИХОТИНСКИЙ