

АУДИТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ БАНКОВ И НЕБАНКОВСКИХ КРЕДИТНО-ФИНАНСОВЫХ УЧРЕЖДЕНИЙ КАК МЕРА ПОВЫШЕНИЯ КАЧЕСТВА НОРМАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ

С.Ю. Воробьев

ОАО «Банковский процессинговый центр», Минск, Беларусь

Концепцией обеспечения кибербезопасности в банковской сфере, утвержденной постановлением Национального банка Республики Беларусь от 20.11.2019 № 466, декларируется направление развития в части придания стандартам информационной безопасности статуса технических нормативных правовых актов, обязательных для соблюдения всеми субъектами банковской сферы, что потребует внесение изменений в Банковский кодекс Республики Беларусь (реализация направлений методологического обеспечения деятельности по обеспечению кибербезопасности в банковской сфере позволит усовершенствовать действующее регулирование в данной области). После придания стандартам информационной безопасности статуса технических нормативных правовых актов, обязательных для соблюдения всеми субъектами банковской сферы, на постоянной основе будет организован контроль за соблюдением стандартов. Контроль соблюдения стандартов по обеспечению кибербезопасности будет осуществляться как Национальным банком (дистанционный контроль, контроль в рамках проведения аудита, внеплановых проверок), так и банками (контроль со стороны подразделений, ответственных за кибербезопасность, а также контроль в рамках проведения внутреннего аудита).

Концепцией информационной безопасности Республики Беларусь, утвержденной постановлением Совета Безопасности Республики Беларусь от 18.03.2019 № 1, декларируется заинтересованность государства по взаимодействию с IT-компаниями, Интернет-провайдерами, операторами связи и внешними экспертами в обновлении и развитии механизмов выявления угроз информационной безопасности через IT-аудит, мониторинг киберрисков, поиск уязвимостей и актуальных средств защиты, выработку правил поведения в сети Интернет.

В настоящее время требования к проведению аудита информационной безопасности банков банковской системы Республики Беларусь устанавливаются СТБ 34.101.42-2013 (в соответствии с законодательством данный стандарт носит рекомендательный характер), технические требования и правила Национального банка Республики Беларусь ТТП ИБ 2.1-2020 содержат требования к проведению внешнего и внутреннего аудитов информационной безопасности соответственно.

Также банки и небанковские кредитно-финансовые организации проводят аудиты на соответствие требованиям стандартов, которые не являются обязательными для применения на территории Республики Беларусь, однако применяются последними для повышения зрелости бизнес-процессов, например, ИСО 27001, PCI DSS, Программа безопасности пользователей SWIFT. Для совершенствования бизнес-процессов, оценки текущего уровня зрелости управления последними (включая сферу кибербезопасности) банки проводят внутренний (или внешний с привлечением аутсорсера) IT-аудит в соответствии с международным стандартом, устанавливающим требования к защите и контролю за конфиденциальными данными COBIT.

Для организации высококлассного ИТ-менеджмента в кредитно-финансовых учреждениях, повышения качества оказываемых услуг активно применяется ITIL.