УДК 657.6:004

ОСУЩЕСТВЛЕНИЕ АУДИТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ КАК МЕРЫ ПОВЫШЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ БАНКА

Воробьёв Станислав Юрьевич, магистр технических наук,
ведущий специалист ОАО «Банковский процессинговый центр»
Vorobyov Stanislav Yurievich, Master of Technical Sciences,
Leading Specialist of OJSC «Banking Processing Center», stogovo@list.ru

Аннотация. В статье рассказывается о сложной обстановке, сложившейся в настоящее время вокруг Республики Беларусь, в т.ч. в экономической, социальной и информационной сферах. Обоснована необходимость дополнительного контроля со стороны органов управления кредитно-финансовыми учреждениями за состоянием информационных систем (в том числе в части защищенности) посредством осуществления мероприятий аудита информационных технологий, приведены основные нормативные правовые акты (в том числе имеющие рекомендательный характер), закрепляющие проведение аудита ИТ-систем.

Ключевые слова: банк, аудит, кибератака, кредитно-финансовые организации, информационные технологии, информационная безопасность, информационные системы.

Обстановка вокруг Республики Беларусь с учетом окружающих глобальных событий в политических, военных, экономических, социальных и информационных сферах в настоящее время остается сложной. Как было отмечено Главой государства, во всем мире наблюдается рост кибератак, причем в первую очередь атакуются стратегические объекты, государственные органы, предприятия, банковская система – основные пункты жизнеобеспечения любого государства [1]. Особую опасность при этом составляют массированные кибератаки на экономические объекты [2]. Так, вредоносным элементом кибератаки выступает компьютерный код или компьютерная программа.

Банковская система Республики Беларусь является составной частью финансово-кредитной системы Республики Беларусь [3]. В соответствии с Концепцией национальной безопасности Рес-

публики Беларусь, национальными интересами в экономической сфере являются сохранение устойчивости национальной финансовой и денежно-кредитной систем [4]. Банковские учреждения крайне активно осуществляют свою деятельность в киберпространстве, что соответственно вызвало увеличение предоставления цифровых услуг, в том числе дистанционного банковского обслуживания (при которых необходимость нахождения клиента непосредственно в кредитно-финансовом учреждении отсутствует, функции операциониста выполняет сам клиент при помощи компьютера, планшета или смартфона, а банк в свою очередь экономит на необходимости содержания офиса).

ИТ-аудит (аудит информационных технологий) решает комплексную задачу получения актуальной и достоверной информации о текущем уровне качества функционирования информационной (-ых) системы кредитно-финансового учреждения [5]. В том числе результаты аудиторских проверок могут служить фундаментом для формирования перечня рекомендаций по повышению уровня защищенности всей ИТ-инфраструктуры финансового учреждения.

В государственном стандарте СТБ 34.101.42-2013 устанавливаются требования к проведению аудита информационной безопасности банков банковской системы Республики Беларусь (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 проведения внешнего и внутреннего аудитов информационной безопасности соответственно.

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).

Положением о технической и криптографической защите информации, утвержденным Указом Президента Республики Беларусь от 16.04.2013 № 196 «О некоторых мерах по совершенствованию защиты информации», в целях определения соответствия системы информационной безопасности требованиям законодательства, в том числе обязательных для соблюдения технических нормативных правовых актов в сфере технической и криптографической защиты информации закрепляется обязанность владельца критически важного объекта информатизации проводить аудит системы информационной безопасности. Аудит системы информационной безопасности проводится владельцем данного объекта информатизации не позднее чем через год после завершения мероприятий по созданию системы информационной безопасности и далее ежегодно. Порядок аудита систем информационной безопасности критически важных объектов информатизации регламентирован Положением о порядке технической и криптографической защите информации, обрабатываемой на критически важных объектах информатизации, утвержденным приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66.

Положением о Национальном центре защиты персональных данных, утвержденным Указом Президента Республики Беларусь от 28.10.2021 № 422 «О мерах по совершенствованию защиты персональных данных», Национальному центру защиты персональных данных предоставлено право проведения на договорной основе добровольного аудита соблюдения операторами (уполномоченными лицами) требований законодательства о персональных данных.

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.

Также банки и небанковские кредитно-финансовые учреждения проводят аудиты на соответствие требованиям стандартов, которые не являются обязательными для применения на территории Республики Беларусь, однако применяются последними при выполнении бизнес-процессов, например: ИСО 27001 (международный стандарт по информационной безопасности), PCI DSS (стандарт безопасности данных индустрии платёжных карт), Программы 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 (Control Objectives for Information and related Technology – контрольные цели для технологии обработки информации). COBIT включает набор лучших методов защиты и контроля за конфиденциальной информацией, соответствующую метрику, чтобы количественно оценить эффективность мер, обеспечивающих ее безопасность, и тесты для проверки. Для организации высококлассного ИТ-менеджмента в кредитно-финансовых учреждениях, повышения качества оказываемых услуг активное применяется ITIL (Information Technology Infrastructure Library - библиотека инфраструктуры информационных технологий) - общепризнанный набор рекомендаций, призванный помочь организациям максимально эффективно использовать ИТ путем согласования ИТ-услуг с бизнес-стратегией).

Республика Беларусь находится в сложных окружающих условиях, в том числе в экономической и информационной сферах с продолжающимися попытками кибератак на кредитно-финансовые учреждения. Для оценки функционирования информационных систем банка, в том числе уровня их защищенности необходимо проведение аудита(-ов) информационных технологий. Осуществление ИТ-аудитов закреплено как в национальном законодательстве (в основном проверка состояния ИБ и организации защиты персональных данных), так и в международных стандартах. ИТ-аудит состоит из ряда этапов и предполагает анализ текущего состояния ИТ-технологий, системы информационной безопасности и киберустойчивости, что позволит вывести оценку зрелости процессов ИТ в кредитно-финансовых учреждениях (в том числе и по вопросам информационной безопасности) на более высокий уровень.

Список использованных источников

1. Совещание по теме кибербезопасности [Электронный ресурс] Официальный Интернет-портал Президента Республики Беларусь. - Режим доступа : https://president.gov.by/ru/events/soveshchanie-po-teme-kiberbezopasnosti. – Дата доступа : 06.03.2023.

2. Встреча с руководящим и оперативным составом органов государственной безопасности [Электронный ресурс] Официальный Интернет-портал Президента Республики Беларусь. - Режим доступа : https://president.gov.by/ru/events/vstrecha-s-rukovodyashchim-i-operativnym-sostavom-organov-gosbezopasnosti. – Дата доступа : 06.03.2023.

3. Банковский кодекс Республики Беларусь [Электронный ресурс]: 25 октября 2000 г., № 441-З: принят Палатой представителей 3 октября 2000 года.: одобрен Советом Республики 12 октября 2000 года.: в ред. Законов Республики Беларусь от 11.11.2021 N 128-З // онлайн-сервис готовых правовых решений по бухучету, налогообложению и праву для бухгалтеров, юристов, руководителей ilex.by / ООО «ЮрСпектр». – М., 2022.

4. Концепция национальной безопасности Республики Беларусь [Электронный ресурс]: Указ Президента Респ. Беларусь, 9 нояб. 2010 г., № 575 // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа : https://pravo.by/document/?guid=2012&oldDoc=2010-276/2010-276(005-026).pdf&oldDocPage=1. – Дата доступа : 06.03.2022.

5. Грекул, В.И. Аудит информационных технологий: учебник для вузов/ В.И. Грекул // М.: Горячая линия – Телеком, 2020. – 154 с.

6. Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Аудит информационной безопасности банков = Інфармацыйныя тэхналогіі і бяспека. Забеспячэнне інфармацыйнай бяспекі банкаў Рэспублікі Беларусь. Аўдыт інфармацыйнай бяспекі банкаў : СТБ 34.101.41-2013. - Введ. впервые. – Минск: Белорус. гос. ин-т стандартизации и сертификации, 2014. – 9 с.