

# Гайки наготове

О том, что думают и, главное, планируют регуляторы и законодатели в области кибербезопасности по неутешительным итогам первого полугодия 2024-го, можно было услышать от них самих



Текст  
**ВАДИМ ФЕРЕНЦ,**  
ОБОЗРЕВАТЕЛЬ «Б.О.»

**К**акое-то время назад эксперты ИБ-рынка полагали, что наиболее радикальными шагами второй половины 2024 года в сфере ИБ станут два документа. Во-первых, второе чтение (и возможное принятие в третьем) в Госдуме пакета законопроектов № 502104-8 и № 502103-8, внесенных на рассмотрение сенатором **Артемом Шейкиным** и депутатом Госдумы **Александром Хинштейном**, касающихся изменения КоАП и ужесточения штрафов за утечки персональных данных (ПДн). Во-вторых, вступивший в силу 25 июля 2024 года 161-ФЗ «О внесении изменений в ФЗ “О национальной платежной системе”», направленный на предотвращение осуществления переводов физлицами, находящимися под воздействием мошенников, а также на активизацию борьбы с дропперами.

Один из возможных путей решения проблемы «дырявых» ИТ-систем виделся в скорейшем принятии Закона о банковском аутсорсинге и облачных вычислениях. Однако он наглухо застрял в Госдуме перед вторым чтением. Банк России активно борется за его продвижение, но конкретных сроков принятия назвать никто не может.

Однако масштаб бедствия и его острый социальный характер заставил и законодателей, и Банк России, что называется, «применить власть» и начать закручивать гайки, причем не кому-нибудь, а прежде всего банкам из списка топ-10.

## Законодательные новации

«Законодатели видят проблемы и активно реагируют», о чем подробно рассказала 4 июля 2024 года в рамках форума Data Day 2024 **Ирина Данилина**, советник председателя экспертного совета при Комитете по финансовому рынку Госдумы.

«За первые три месяца 2024 года количество инцидентов, связанных с утечками конфиденциальной информации, составило 334 против 146 за аналогичный период прошлого года.

Рост в 2,3 раза. И это только по тем инцидентам, которые стали публичными, например, как громкий случай утечки ПДн у сервиса "СберСпасибо" в 2023 году. Понятно, что ситуация требует объединения усилий экспертов Государственной Думы и Совета Федерации», — заявила Ирина Данилина.

Очевидно, речь идет об «обелении» рынка ИБ, разработке механизмов предания гласности случившихся инцидентов, а также о возмещении причиненных убытков пострадавшим. А начать планируется с финансового сектора в силу его максимальной инфраструктурной и технологической готовности к этим инициативам.

В центре внимания депутатов обеих палат парламента в этой связи находится модернизация института страхования киберрисков. Совет Федерации готовит законопроект «Об обязательном страховании киберрисков операторами ПДн», которые будут обязаны либо создавать обязательный денежный фонд для компенсации вреда гражданам, чьи данные были украдены, либо страховать этот риск.

Сенатор Артем Шейкин заявил в этой связи: «Создать в России рынок страхования от киберугроз — необходимая задача, подлежащая скорейшему исполнению».

### ГОСТ 57580.1 подлежит переизданию

Заместитель директора департамента информационной безопасности Банка России **Андрей Выборнов** и главный инженер отдела ИБ и киберустойчивости финансовых технологий этого же департамента **Константин Стародубов** в начале июня 2024 года от имени Банка России на конференции «ИБ финансовых организаций в текущих условиях» совместно с Ассоциацией российских банков (АРБ) подвели некоторые итоги, а также скорее огорчили, нежели порадовали коллег теми планами, которые регулятор самым активным образом продвигал все первое полугодие 2024-го.

Андрей Выборнов был предельно откровенен. По его словам, история с пакетом ГОСТ 57580 рассчитана на добросовестное применение, суть которого заключается в том, что банк должен сам осознавать свои собственные риски. На этом основании должна происходить корректировка его деятельности со стороны топ-менеджмента. Таким образом, базовая идея документа заключена в организации непрерывного мониторинга рисков на основе достоверной информации, а также в адекватном реагировании на нее. Положение ЦБ № 716-П, дополняющее ГОСТ, написано таким образом, чтобы руководство банков было заинтересовано в получении объективных показателей операционных рисков.

Если механизм доведения системой внутреннего контроля и аудита до топ-менеджмента достоверной информации о рисках не работает, сознательно или нет, то вся эта идея превращается в профанацию. Что, собственно, и происходит.

«Мы видим, что в ряде банков формально все выполняется. Но по факту многое там необъективно. Что в этой ситуации делать Банку России? А ничего не остается, как самому соответствующим образом оценивать систему управления операционным риском на основе существующего Указания ЦБ № 4336-У «Оценка экономического положения банка», которое сейчас пересматривается профильными департаментами и готовится к публикации. Готовятся и обновленные методические рекомендации (МР), касающиеся показателей по фроду, включая кредитное мошенничество, и операционной надежности. Будет не только закреплена четкая номенклатура этих показателей, но и установлены их минимальные числовые значения. Надежда на их добросовестное самостоятельное установление банками, согласно 716-П, должна быть подкреплена мягким регулированием. А оценивать качество управления рисками будем не только по качественным показате-

лям, но и по количественным в интеграции с 4336-У», — заявил Андрей Выборнов.

По словам докладчика, Банк России более всего волнует такой показатель управления операционным риском, как уровень фрода (операции без согласия клиента) в кредитных организациях, входящих в топ-10, как на стороне банков-плательщиков, так и на стороне банков, которые «обслуживают» дропов.

Проверки показывают, что далеко не везде все «аккуратно». Наиболее типичный пример: игнорирование Положения № 716-П, заключающееся в отказе в приеме заявлений от клиентов, что занижает показатели фрода и создает иллюзию благополучия. Банк России постоянно указывает на это, считая, что права клиентов должны быть защищены в обязательном порядке, а сама проблема уже носит социальный характер.

Другой показатель, который регулятор держит под особым контролем, характеризует сферу выдачи кредитов, поскольку ущерб от кредитного фрода уже превышает остальные потери. Поэтому борьба с мошенничеством при выдаче кредитов должна стать в перспективе частью Положения № 716-П, а соответствующий показатель будет жестко контролироваться.

### Ближайшие планы Банка России

«Над чем конкретно сейчас работают эксперты регулятора: над проблемой концентрации риска в отдельных организациях, не поднадзорных Банку России, но от деятельности которых существенно зависит функционирование финансового рынка в целом. В их числе облачные провайдеры и ключевые вендоры. На изучении этого вопроса и понимании сути этих рисков будут сконцентрированы максимальные усилия регулятора на горизонте до двух лет. Пока «стройных идей», как подойти к этому вопросу, не выработано», — сообщил Андрей Выборнов.

Константин Стародубов добавил к сказанному: «Создана рабочая группа «Ревизия положений стандартов ГОСТ № 57580.1 и 57580.2». В первом документе расширен субъектный состав за счет финтех-компаний, переработан процесс «Контроль целостности и защищенности IT-инфраструктуры» и т.д. Во втором — уточнен давно наболевший критерий «независимости» по отношению к проверяющим организациям. Второй блок задач: разработка МР, касающихся тестирования на проникновение и анализа уязвимостей. Основные цели этого документа — оценка уровня реальной защищенности объектов информационной архитектуры организаций финансового рынка, а также обеспечение доверия к ним, включая входящие в список критичной архитектуры».

БО