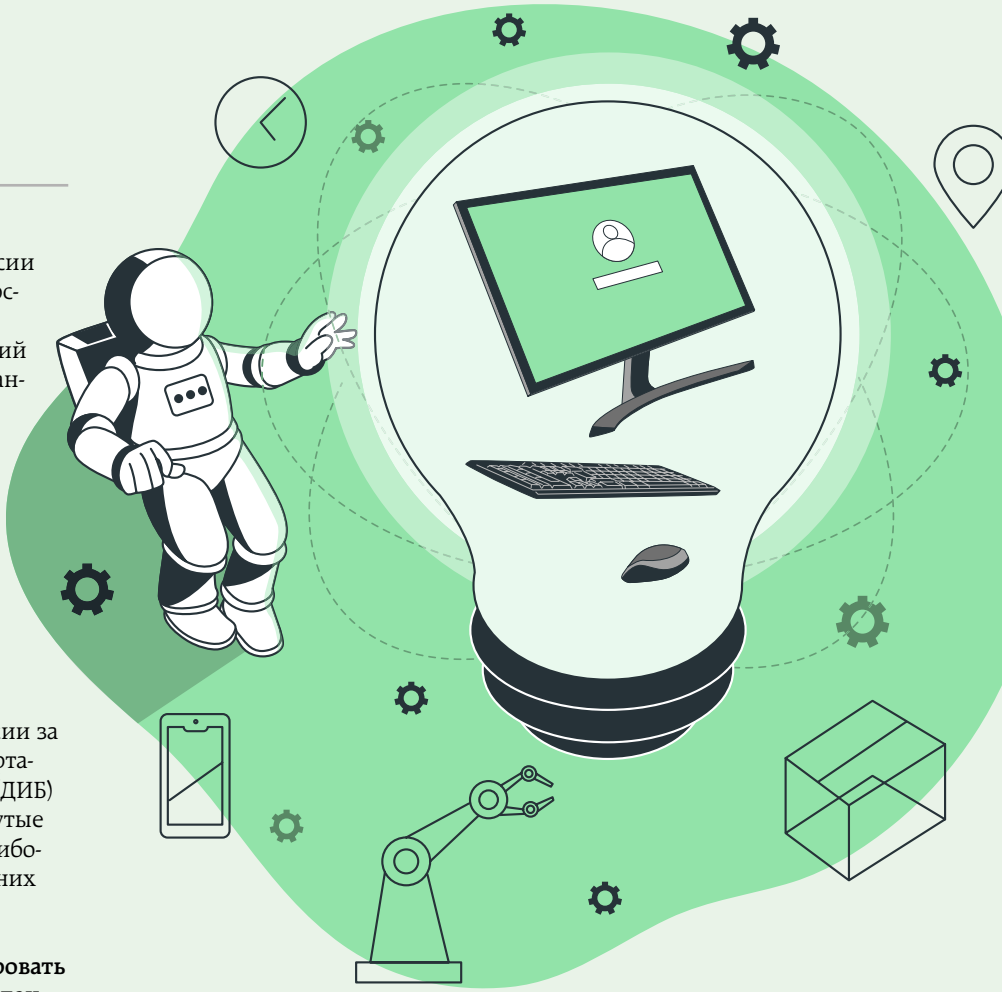
Киберучения свет

Проблематика обеспечения ИБ в условиях внедрения риск-ориентированного подхода к обеспечению кибербезопасности продолжает вызывать методологические затруднения у участников финансового рынка

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



Ассоциация банков России (АБР) и Ассоциация российских банков (АРБ) прилагают массу усилий для разъяснения финансовому сообществу тонкостей быстро изменяющегося регулирования в области ИБ. Сложностей добавляет практика использования средств криптографической защиты информации (СКЗИ) в условиях импортозамещения и движения отрасли в сторону IT-аутсорсинга.

Обращения АБР к ДИБ

В начале апреля 2024 года из Банка России за подписью заместителя директора Департамента информационной безопасности (ДИБ) **Андрея Выборнова** поступили развернутые разъяснения на два обращения АБР. Наиболее актуальная информация одного из них приведена ниже:

— Планирует ли Банк России инициировать пересмотр требований к СКЗИ, утвержденных ФСБ, чтобы разрешить применение технологий аппаратной виртуализации и облачной модели оказания услуг в отношении ряда ПО?

— HSM-модуль останется в банках: проектом Федерального закона № 404786-8 «О внесении изменений в отдельные законодательные акты Российской Федерации» планируются поправки в действующее законодательство, направленные на снятие ограничений, связанных с передачей охраняемых законом видов тайн на аутсорсинг. Предполагается, что положения законопроекта будут распространяться в том числе на случаи использования организациями финансового рынка облачных услуг по обеспечению сервисов информационной безопасности.

С учетом широко признанных практик применение кредитными организациями облачного решения, реализующего функции аппаратного модуля безопасности информационной инфраструктуры платежной системы (HSM-модуля), на текущем этапе не рассматривается в качестве допустимого сценария аутсорсинга в рамках осуществления переводов денежных средств.

— Допустимо ли для финансовой организации выполнение требований Положений № 683-П и № 757-П не в полном объеме, если данный факт не повлияет на достижение нормативно установленного уровня соответствия требованиям к защите информации?

— Положения № 683-П и № 757-П необходимо выполнять в полном объеме: требование о реализации уровня защиты информа-

ции, предусмотренного ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций…» является одним из набора требований, установленных Положением Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» и Положением Банка России от 20.04.2021 № 757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».

Выполнение данного требования не влияет на необходимость выполнения иных требований, установленных указанными нормативными актами Банка России.

— В какие сроки Банк России планирует пересмотреть требования разд. 7.4 «Профиля защиты прикладного ПО…» для адаптации к современным практикам гибкой разработки кода?

— В настоящее время ДИБ не располагает достаточными данными относительно практики применения положений разд. 7.4 «Профиля защиты». В целях разработки и внедрения безопасных программных продуктов при сохранении гарантированного и достаточного уровня защищенности прикладного программного обеспечения автоматизированных систем и приложений, используемых при осуществлении финансовых (в том числе банковских) операций, ДИБ рекомендует использовать новый раздел документа.

При этом в рамках сопровождения «Профиля защиты» ДИБ ориентируется на выпускаемые, а также планируемые к выпуску национальные стандарты РФ по разработке безопасного ПО, работа над которыми ведется в техническом комитете по стандартизации № 362 «Защита информации», а также на международные стандарты и лучшие практики.

В связи с изложенным пересмотр разд. 7.4 «Профиля защиты» в части расширения случаев применения, а также рассмотрение возможности использования оценки с учетом положений разд. 7.4 «Профиля защиты» для допуска ПО к использованию наряду с ПО, включенным в реестр Минцифры, планируется осуществлять после апробации применения финансовыми организациями подходов к безопасной разработке ПО и приложений, согласно перспективным правовым условиям.

Наиболее интересный вопрос из состава второго запроса АБР был связан с тем, что 25 июля 2024 года вступает в силу Закон № 369-ФЗ, который вносит существенные изменения в процедуру антифрода в кредитных организациях. Банкиров интересовали детали протокола взаимодействия с АИС «Фид-Антифрод». На этот и другие вопросы также был получен информативный ответ.

Круглый стол по ИБ от АРБ

В апреле 2024 года в АРБ прошел Круглый стол «Информационная безопасность в финансовом секторе — 2024», на котором Андрей Выборнов получил возможность лично подробнее остановиться на направлениях развития информационной безопасности кредитно-финансовой сферы на 2023–2025 годы, обозначенных в соответствующей Стратегии.

В Банке России считают уместным для устранения разночтений в области действующих и разрабатываемых регулятором нормативных актов еще раз вспомнить о целях своей деятельности в области ИБ. Их всего три:

1. Защита прав потребителей финансовых услуг и повышение уровня доверия к цифровым технологиям.
2. Создание условий для безопасного внедрения финансовыми организациями цифровых и платежных технологий, а также обеспечения технологического суверенитета.
3. Обеспечение контроля рисков информационной безопасности, операционной надежности для непрерывности предоставления финансовых услуг.

В рамках первой цели основными направлениями развития являются противодействие совершению операций без согласия клиентов и социальной инженерии, противодействие компьютерным атакам, а также повышение финансовой грамотности. Вступающий в силу 25 июля 2024 года Закон № 369-ФЗ, уже упоминавшийся выше, должен дополнить меры, предусмотренные Законом № 161-ФЗ «О национальной платежной системе». Новшествами станут «двухдневный период охлаждения» при попытке перевода денег заведомо мошенникам, обязанность банков по возврату денег физическим лицам, если банк не выполнил действия, предусмотренные Законом № 161-ФЗ перед переводом денежных средств, а также появление списка мер, направленных против дропперов. Регулятор особо обращает внимание на рост случаев кредитного фрода, с чем намерен жестко бороться.

Вторая цель реализуется в том числе рядом мер, связанных с запуском цифрового рубля и обеспечением безопасности участников пилотного проекта с соответствующей IT-платформой в рамках Положений Банка России № 820-П и № 733-П, принятых в конце 2023 года. Еще одним приоритетом является проблематика биометрической идентификации и аутентификации клиентов, что нашло свое отражение в появлении СТО БР БФБО-1.8-2024, принятом и введенном в действие Приказом Банка России от 28.02.2024 № ОД-326. На финальной стадии визирования находятся методические рекомендации по практикам применения этого СТО.

Что касается обретения технологического суверенитета, то сохраняются требования к крупным банкам по переводу критичного ПО на отечественные аналоги до 1 января 2025 года, а на доверенные программно-аппаратные комплексы (ПАК) — до 1 января 2030 года.

Третья цель достигается путем «погружения» рисков ИБ в состав операционных рисков в соответствии с Положением № 716-П. Значимыми направлениями приложения усилий являются развитие Reg- и Sup-Tech проектов, IT-аутсорсинга, а также риск-профилирование. Критерием успешности усилий станут итоги регулярных киберучений. Б.О