# Индустрия предотвращения

## Материалы онлайн-конференции НАУФОР «Кибербезопасность некредитных финансовых организаций 2024»

Фотографии **Павел Перов**

Участники: Вадим Гриценко (начальник управления информационной безопасности ПАО «Московская биржа»), Андрей Киселев (директор по информационной безопасности АО «НРК – Р.О.С.Т.», АО «НРК Фондовый рынок»), Александр Луганцев (начальник отдела информационной безопасности АО «ВТБ Специализированный депозитарий», Александр Плоткин (консультант Центра координации обеспечения технологического суверенитета финансового рынка Банка России), Константин Стародубов (консультант Управления методологии и стандартизации информационной безопасности и киберустойчивости Банка России), Антон Чернодед (руководитель направления Управления методологии и стандартизации информационной безопасности и киберустойчивости Банка России), эксперты и члены рабочей группы Комитета по экономической и информационной безопасности НАУФОР.

Модератор: Михаил Шабанов (председатель Комитета по экономической и информационной безопасности НАУФОР).

### I часть

**Особенности и практика реализации требований Положения Банка России от 14 ноября 2021 года № 779-П**

**Михаил Шабанов.** Добрый день, уважаемые участники конференции!

Мне очень приятно открывать уже ставшую традиционной ежегодную конференцию по информационной безопасности для некредитных финансовых организаций. Тема нашей конферен-

ции — кибербезопасность. Модератором буду я, Михаил Шабанов, председатель Комитета по экономической и информационной безопасности НАУФОР.

С учетом тематики конференции предлагаю начать с обсуждения Положения Банка России № 779-П от 14 ноября 2021 года. Слово для выступления хочу предоставить Антону Игоревичу Чернодеду, руководителю направления Управления методологии и стандартизации, информационной безопасности и киберустойчивости Департамента информационной безопасности Банка России.

Антон Игоревич, пожалуйста, вам слово.

**Антон Чернодед.** Коллеги, здравствуйте!

Мое выступление посвящено вопросам операционной надежности. Просьба включить презентацию. Спасибо.

Я коснусь основных вопросов, которые урегулированы в рамках Положения № 779-П, также коснусь основных моментов, на которые стоит обратить внимание спустя три года применения данного Положения.

Финансовые организации должны обеспечить операционную надежность в условиях реализации информационных угроз. В соответствии с требованиями 779-П источником риска для операционной надежности являются компьютерные атаки, соответственно, вся инфраструктура строится вокруг них.

Первый и, пожалуй, один из самых основополагающих пунктов — это идентификация перечня используемых объектов информационной инфраструктуры (мы его более подробно коснемся позже).

Второй пункт — оценка рисков операционной надежности по направлению обеспечения технологического сувере-

нитета, которое в нынешних условиях достаточно актуально.

Третий пункт — управление изменениями критичной архитектуры. Четвертый пункт — выявление инцидентов операционной надежности и реагирование на них, а также восстановление.

Пятый пункт — взаимодействие с поставщиками IT и облачных услуг. Мы из года в год, уже примерно на протяжении трех лет, проводим опрос финансовых организаций: как достаточно крупных, которые подпадают под усиленный уровень защиты, так и небольших, которые должны соответствовать минимальному уровню защиты. Спрашиваем, как они взаимодействуют с поставщиками услуг, как оценивают риски, как эти риски регулируют. В опросе, который проводился в августе 2024 года, был достаточно подробный перечень вопросов, в будущем планируется это все перенести в требования Банка России.

И шестое — это тестирование операционной надежности технологических процессов.

Коснемся более подробно идентификации перечня объектов информационной инфраструктуры. У Банка России как регулятора в части запроса информации об объектах инфраструктуры от поднадзорных организаций имеются четыре цели.

Первая цель: выяснить, какие уязвимости есть у программного обеспечения, серверного оборудования и так далее, которое использует финансовая организация.

Вторая: планы импортозамещения. Этого вопроса более подробно коснется один из последующих докладчиков со стороны Банка России.

Третья цель: информирование об инцидентах (чтобы было понимание, на какие объекты информационной инфраструктуры была совершена компьютерная атака).

И четвертая цель: единообразный учет объектов информационной инфраструктуры. Чтобы финансовые организации могли вести учет в одном формате на постоянной основе и при необходимости использовали эти сведения в своей деятельности либо предоставляли их в Банк России.

В этих целях мы год назад разработали методические рекомендации 18-МР, где достаточно подробно описано, какие сведения об объектах Банк России хотел бы иметь. Там содержится порядка 34 атрибутов (достаточно большой перечень), но есть послабления для небольших организаций. То есть, 34 атрибута являются обязательными для финансовых организаций, которые подпадают под усиленный или стандартный уровни защиты информации. Для финансовых организаций, которые подпадают под минимальный уровень защиты информации, перечень атрибутов уменьшен до 14. Эти сведения на регулярной основе, ежеквартально необходимо представлять в Банк России в рамках подотчетности по операционной надежности. Для каждого вида деятельности есть своя форма отчетности. Если кредитная организация совмещает свою деятельность с финансовой деятельностью, то все делается в рамках одной формы отчетности, 72-й.

Мы получаем данные формы отчетности от некредитных финансовых организаций и от кредитных организаций поменьше уже достаточно долго, есть возможность подвести итоги сбора.

Организации представляют эти данные по-разному. Есть типовые ошибки. Необходимо отметить следующее: чтобы в дальнейшем эти сведения можно было обработать, в том числе автоматизировано, необходимо корректное заполнение отчетности. Если предусмотрено 34 атрибута, то должно быть соответствующее количество разделителей. Если количество разделителей недостаточно, то автоматизированная обработка этих сведений усложняется. Поэтому необходимо проставлять все разделители.

Если в рамках какого-то атрибута сведений нет (либо организация подпадает под минимальный уровень защиты информации и этот атрибут ей необязателен), то этот пункт организация просто пропускает, но, тем не менее, разделитель необходимо поставить.
В ряде атрибутов также предусмотрено предоставление данных в рамках, например, различных бизнес-функций: то есть атрибут один, но нужно перечислить несколько бизнес-функций.

В дальнейшем Банк России планирует усилить работу по данному направлению, чтобы финансовые организации представляли для последующей обработки более чистые и корректные данные.

Кроме представления форм отчетности, эти сведения представляются через автоматизированную систему АСОИ ФинЦЕРТ в рамках информирования об инцидентах либо могут быть запрошены при проверочных мероприятиях. То есть финансовой организации целесообразно вести учет своих объектов информационной инфраструктуры в соответствии с данными рекомендациями, это в дальнейшем облегчит взаимодействие с регулятором.

Следующий слайд. Также достаточно важным блоком операционной надежности является управление рисками. Мы разделили данное направление на пять пунктов, которые вам всем прекрасно знакомы.

Первый пункт: определение целевых значений показателей, на которые финансовая организация ориентируется. В дальнейшем по данному направлению планируется дополнительная работа со стороны регулятора. Мы видим, что организации оценивают свои риски поразному. Считаю достаточно критичным указывать все-таки сильные целевые значения. Кто-то намеренно их занижал, фактически создавая ситуацию, в которой организация может простаивать на постоянной основе и, соответственно, у нее инцидент операционной надежности никогда не произойдет. Это непра-

вильный подход, и Банк России в дальнейшем будет с этим работать.

Второе — это организация контроля фактических значений данных показателей и доведение этой информации до органов управления финансовой организации. Вся структура должна знать, что внутри нее происходит с операционной надежностью.

Третье — это организация трех линий защиты, но только для тех финорганизаций, в которых (в соответствии с другими нормативными актами) предусмотрена система управления операционным риском.

Четвертый пункт — ведение базы событий операционного риска либо инцидентов операционной надежности. Пятый пункт — реализация мер по защите информации и операционной надежности.

В совокупности все эти требования направлены на то, чтобы организация знала свою информационную инфраструктуру, знала, какие риски для нее актуальны, умела этими рисками управлять и представлять эти сведения регулятору для последующих надзорных мероприятий.

Доклад закончил, готов к дискуссии.

**Михаил Шабанов.** Большое спасибо, Антон Игоревич.

Дискуссию мы продолжим после того, как выступит Александр Луганцев, начальник отдела информационной безопасности АО «ВТБ Специализированный депозитарий». Тема его выступления: «Грабли информбезопасности, или как наладить в НФО процессы операционной надежности».

Александр, пожалуйста, вам слово.

**Александр Луганцев.** Добрый день, уважаемые коллеги по ту сторону экрана! Добрый день, все находящиеся здесь!

Доклад мой будет как бы продолжением темы предыдущего докладчика, но более, скажем так, применительно к практике. За 15 минут невозможно раскрыть все особенности внедрения в организации Положения № 779. Я постараюсь раскрыть тот подход, к которому склонились мы при реализации всего лишь одного направления. Остальные затрону как бы попутно.

В 2021 году вышло Положение по опернадежности для некредитных организаций. В связи с этим возникла масса вопросов, как выполнять все предписанное Положением в организационном плане. Почему-то вдруг все решили, что это тема исключительно для сотрудников подразделения информационной безопасности. Мы на первом этапе все это безобразие возглавили, с единственной целью доказать, что в реализацию Положения должны быть вовлечены практически 90% нашего доблестного коллектива. Потом мы это доказали, но руководящим и направляющим у нас все-таки стал специалист, который возглавляет направление операционной надежности. Он и раздает задачи всем сотрудникам.

Сейчас вышло 7-МР, которое более или менее конкретизирует все эти подходы. Этот документ, я считаю, снял большинство вопросов.

Теперь давайте перейдем к практической теме. Когда мы только начали изучать тему, то собрали инициативную группу, провели порядка трех-четырех совещаний. При обсуждении Положения возникло (я специально перепроверил) 67 вопросов, на которые мы постарались ответить. Здесь за аксиому приняли, что все мы люди умные, с высшим образованием, поэтому как решим, так и будет. А если мы что-то не решили или решили неправильно, то нас впоследствии поправят.

Создали рабочую группу по реализации данного Положения, на первом этапе назначили ответственного за эту реализацию. В основном были разработаны организационно-методические документы, которые регламентируют всю эту деятельность. Это заняло значительное количество времени.

Первое направление: назначение ответственных. Ответственные у нас были назначены, как я говорил, практически по 70% направлений [деятельности компании]. Потом мы разделили [сферу действия] П-779 на 15 процессов, и каждый из 15 процессов получил своего «вождя», который отвечает в своей зоне за реализацию данных процессов.

Затем были приняты три документа с приложениями, которые регламентируют то или иное направление. За основу был взят сам основной документ П-779, он был переработан применительно к специфике нашей организации, было разработано Положение по реализации в компании операционного риска, с приложениями. В одном из приложений как раз, как говорил предыдущий докладчик, содержится описание выделения тех информационных ресурсов, которые подпадают под действие 779, причем это выделение доказательное, обоснованное и понятное для всех. Мне бы хотелось об этом рассказать.

Исходили мы из того, что при прочтении нашего документа даже у человека, который не имеет никакого отношения к информационной безопасности, не должно остаться вопросов, почему те или иные информационные системы попали под действие Положения № 779 и почему к ним применяются требования по управлению операционным риском.

Сперва мы выделили информационные системы, которые обрабатывают ту информацию, используя которую, наша компания оказывает финансовые услуги. Просто перечислили, какие подразделения используют этот функционал в своей повседневной деятельности и, соответственно, являются ответственными.

Затем мы перешли конкретно к каждой информационной системе и определили, в каком технологическом процессе задействована та или иная информационная система (можно употребить термин «программно-аппаратный комплекс»). Далее мы определи-

ли информацию, которая циркулирует между данными информационными системами.

Небольшое отступление. При разработке этого документа мы старались увязать его с другими требованиями, которые также обозначены в Положении № 779. То есть, допустим, мы должны учитывать взаимозависимости между подразделениями внешними и внутренними. Исходя из этого, надо понять, кто какую информацию использует, какое подразделение от какого подразделения зависит, определить эти зависимости. Также попутно определяем уровень конфиденциальности циркулирующей информации.

Далее мы анализируем систему электронного документооборота. Здесь уже следует понять, через какие технологические участки проходит информация, которую формирует наш клиент для проведения той или иной финансовой операции, какие средства информационной системы на каждом технологическом участке задействованы. Все это сводим в табличную форму.

Теперь приведу пример конкретного подразделения, конкретного технологического процесса. Для примера я взял подразделение контроля пенсионных фондов. Здесь мы схематично указали, каким образом информация от клиента доходит до исполнителя, возвращается обратно, какие решения при этом принимаются, какие решения контролируются и с использованием каких средств. Это логическая схема, к ней еще идет описание, то есть каждое движение разноцветной стрелочки описано обыкновенным, нормальным человеческим языком. Каждый может прочитать и понять, как это все происходит на самом деле.

Далее мы разбиваем процесс уже на более конкретные участки деятельности: на каком конкретно технологическом участке выполняются те или иные действия. Опять же, все это сведено в таблицу.

Вот тут мы пошли еще дальше. То есть мы взяли конкретный технологи-

ческий процесс, далее разбили его на технологические этапы и расписали для каждого этапа, какие программно-аппаратные комплексы принимают участие в работе на этом этапе.

Что мы можем понять из данной схемы? Во-первых, какие программно-аппаратные средства и операционные системы участвуют и зачем. Здесь мы сразу понимаем, на каких этапах нужно обеспечить отказоустойчивость, с использованием какого оборудования, канала какой пропускной способности. Далее учет уязвимостей: как их закрывать, на что обратить особое внимание.

Так мы подошли к каждому технологическому процессу. Далее свели все это в одну таблицу и описали. Получился очень легкий и читабельный документ, изучая который, всем все становится ясно и понятно.

Далее мы определили каждому процессу внешние и внутренние взаимосвязи. За основу были взяты целевые показатели, у нас их считают, соответственно, операционисты. Мы подошли как? есть какая-то информационная система, какой-то информационный процесс, который технологически обеспечивает выполнение конкретных финансовых операций. Следует проанализировать, что случится, если этот процесс остановится на час, остановится на 12 часов, остановится на одни сутки, остановится на период более суток. Что мы в каждой ситуации теряем, какой риск в каждой ситуации может реализоваться. С конкретными мерами, описанием нештатных ситуаций.

Ну и дальше в приложении мы уже расписали те контроли, которые необходимо осуществлять, в виде таблицы-приложения к каждому существующему процессу.

По объему этот документ получился в районе 120–130 страниц. Разрабатывал его отдел информационной безопасности с привлечением операционистов, они нам очень сильно помогли, и с привлечением системы управления риском.

Доклад закончил, спасибо за внимание.

**Михаил Шабанов.** Большое спасибо, Александр, за очень интересную презентацию.

Коллеги, эксперты, пожалуйста, если есть комментарии, можно сейчас высказаться.

Антон Игоревич, тогда короткий вопрос у меня, касающийся подхода, который изложил Александр в своей презентации. Как видится ситуация Департаменту информационной безопасности Банка России, вы согласны с таким подходом?

**Антон Чернодед.** Возражений по данному подходу у нас нет, он имеет право на существование, там достаточно подсвечены основные моменты, которых требует 779 Положение.

**Михаил Шабанов.** Спасибо.

Если нет вопросов, то после перерыва перейдем ко второй части.

## II часть

**От сертификации и оценки соответствия по ОУД-4 до безопасной разработки ПО**

**Михаил Шабанов.** Прежде чем перейти к обсуждению второй темы, я бы хотел напомнить о том, что с 20 декабря 2024 года вводится в действие ГОСТ 56939 от 2024 года «Защита информации, разработка безопасного программного обеспечения. Общие требования». Стандарт устанавливает общие требования к содержанию и порядку выполнения работ, связанных с созданием безопасного программного обеспечения, и устранению выявленных недостатков, в том числе уязвимостей.

Слово предоставляется Константину Стародубову, консультанту Управления методологии и стандартизации информационной безопасности и киберустойчивости Департамента информационной безопасности Банка России.

Константин, пожалуйста, вам слово.

**Константин Стародубов**. Добрый день, уважаемые коллеги! Рад вас приветствовать.

Сегодня я расскажу, как перейти от сертификации и оценки соответствия по ОУД-4 к безопасной разработке, и что сделано Банком России в целом для данного процесса.

Практически во всех нормативных документах Банка России есть требование, что прикладное программное обеспечение автоматизированных систем и приложений, распространяемых клиентам для совершения ими действий, или ПО, обрабатывающее защищаемую информацию на технологических участках, используемых для приема электронных сообщений, должно проходить развилку: сертификацию либо по ОУД-4, либо по требованиям ФСТЭК в их испытательных лабораториях.

Данные пункты содержатся в 683 Положении «Об информационной безопасности кредитных организаций», 758 Положении Банка России «Об информационной безопасности для некредитных финансовых организаций», в Положении 821-П «Об информационной безопасности в денежных переводах» и в Положении 808-П «Об информационной безопасности в сфере финансовых рынков». Думаю, все уже к ним привыкли.

Чтобы определить подходы к данным направлениям, Банк России разработал «Профиль защиты прикладного программного обеспечения и автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций». 2 февраля 2022 года на официальном сайте Банка России было размещено информационное письмо, которое сообщает, что оценку соответствия ОУД-4 для кредитных финансовых организаций можно выполнить несколькими способами. Первый способ: выполнение требований по разделу 7.2, который помогает пройти оценку соответствия по ОУД-4

в соответствии с ГОСТ 15408. Второй момент, который поможет выполнить данные требования, — это выстраивание процессов безопасной разработки, которое описано в разделе 7.4 «Профиля защиты».

Безопасная разработка, которая описана в разделе 7.4, поможет организациям финансового рынка, на которые распространяется это требование, закрыть все требования к информационной безопасности, которые существуют в данном пункте. Для этого необходимо выстроить процесс безопасной разработки в каждой организации.

Раздел 7.4 был согласован и одобрен на подкомитете № 1 Технического комитета № 122. В работе этого комитета участвуют многие финансовые организации, и регулятор сделал нормативный документ совместно с ними. Данный документ можно скачать с официального сайта Банка России, он находится в свободном доступе.

Каковы были цели выпуска раздела 7.4 «Профиля защиты»?

Первое: когда в организации происходит быстрый релизный цикл, когда выпускается достаточно много релизов. Тогда 7.4 будет работать.

Второе: когда есть задача повысить защищенность разрабатываемого ПО и снизить количество уязвимостей, которые в нем находятся.

Третье: когда есть потребность сделать обеспечение информационной безопасности неотъемлемой частью разработки.

Раздел 7.4 применяется ко всему жизненному циклу разработки.

Какой подход мы заложили в разделе 7.4 «Профиля защиты»? Это переход от ОУД (требований по безопасности, которые изложения в пункте 7.2 «Профиля защиты») к требованиям по организации процесса безопасной разработки при наличии конкретных требований по ИБ, с учетом реальных рисков, специфики разработки и функционирования продукта.

Какие же критерии будут способствовать переходу от требований ОУД и проведения сертификации объекта оценки к сертификации безопасной разработки?

Во-первых, прикладное программное обеспечение и приложения не должны относиться к категории критичных информационных систем. Данное требование было введено умышленно, потому что мы хотим протестировать, как положения раздела 7.4 будут работать в реальных организациях. Хотим собрать большое количество мнений участников финансовых организаций относительно того, как это внедрять, какие есть нюансы, что нужно подкрутить. Об этом я скажу чуть попозже, уже в финале своего доклада.

Второе. Инфраструктура разработки, тестирования, среды постоянной эксплуатации должна соответствовать требованиям ГОСТ 57580.1.

Третье. Должна быть в наличии собственная разработка в соответствии с компетенциями, должно осуществляться постоянное обучение сотрудников по линии информационной безопасности. Эту работу внутри организации следует делать, компетенции сотрудников должны быть достаточны для того, чтобы позволить провести всю безопасную разработку качественно.

Четвертое — наличие необходимых автоматизированных инструментов для создания среды и настройки жизненного цикла.

Пятое — наличие документированного процесса разработки, тестирования и эксплуатации с описанными контролями и проверками по обеспечению ИБ, а также документированного процесса управления версиями и изменениями программно-прикладного обеспечения и приложений.

И последнее: инфраструктурные системы (платформы) и решения по обеспечению ИБ должны быть документированы в достаточном виде. Вышел новый ГОСТ по безопасной разработке, который как раз регламентирует необходимость и объем разрабатываемой документации.

При переходе от ОУД к безопасной разработке в профиле защиты заложен риск-ориентированный подход применения контролей безопасности при разработке и тестировании ППО/приложений и вообще при эксплуатации во всем жизненном цикле.

Здесь идет и определение актуальных требований ИБ и мер защиты, связанных с атаками слабостей (CWE), составлением связанных с CWE уязвимостей (CVE) и уязвимых конфигураций (CPE).

Должен проводиться анализ рисков нарушения информационной безопасности, определение векторов и актуальных атак (CAPEC), а также должен проводиться контроль ИБ при переносах между средами (контроль корректности требований ИБ, автотесты, статический, динамический анализ, пентесты, композиционный анализ и так далее).

При внесении изменений в ППО или приложение должен постоянно проходить мониторинг инцидентов, а также анализ необходимости проведения полного цикла контролей. И постоянно должны внедряться меры по минимизации рисков информационной безопасности.

Как я уже говорил ранее, главным условием перехода на безопасную разработку должно быть наличие обученных специалистов. Профиль защиты предусматривает и описывает роли, которые должны вводиться при таком переходе. Таких ролей две: аналитик ИБ (либо офицер ИБ) и Security Champio №.

Роль аналитика ИБ или офицера ИБ обычно выполняет сотрудник подразделения информационной безопасности, который владеет всей ситуацией в мире и на рынке, знает основные типы угроз, который также может программировать и искать уязвимо-

сти. Такие специалисты достаточно уникальны, при этом они должны быть везде. Поэтому мы допускаем, что один аналитик может работать на несколько подразделений.

Чтобы минимизировать данные риски, в команду вводится роль Security Champio №. Это роль для специалиста с высокой осведомленностью в вопросах информационной безопасности, который является помощником аналитика ИБ и своего рода связующим звеном, который умеет разговаривать на языке информационной безопасности и доводить между командой разработки и аналитиком либо офицером ИБ все необходимые требования.

Дополнительно в профиле защиты сказано, что разработчику необходимо обеспечить подготовку повышения компетенции сотрудников. То есть, должно происходить постоянное обучение. Наш ландшафт информационной безопасности постоянно меняется, необходимо всегда быть в тренде и знать, какие уязвимости и угрозы существуют на текущий момент.

Разработчику необходимо периодически осуществлять пересмотр состава ролей и их обязанностей, чтобы как можно больше участников команды могли обучиться и быть более осведомленными в вопросах информационной безопасности. Мы стараемся внедрить функции безопасности на всех участках жизненного цикла разработки программного обеспечения.

Мы ожидаем внедрения раздела 7.4 в жизненный цикл всех участников финансового рынка. Мы ожидаем, что качество безопасной разработки будет повышено за счет глубокого анализа работы продукта и обучения разработчиков принципам безопасности.

Мы надеемся, что принятие решений в отношении операционных рисков будет происходить коллегиально, с привлечением всех участников процесса внедрения безопасного программного обеспечения.

Также надеемся, что стоимость уязвимостей будет уменьшаться, а скорость их исправления — увеличиваться, благодаря нахождению уязвимостей на более ранних стадиях разработки. И будет непрерывный мониторинг защищенности ППО/приложений, своевременности исправления уязвимостей и управления их обновлениями.

Это то, чего регулятор хотел достичь, когда разрабатывал профиль защиты.

Теперь перейдем к планам. Что касается планов и результатов нашей работы.

Во-первых, Банк России введет разработку методических рекомендаций по тестированию на проникновение и анализ уязвимостей объектов информационной инфраструктуры. Данные методические рекомендации будут описывать подходы к тестированию на проникновение, подходы к классификации и устранению уязвимостей в системе информационной безопасности. Ожидаем, что в первой половине следующего года данные методические рекомендации будут опубликованы на официальном сайте Банка России. Они помогут финансовым организациям стандартизировать подход к проведению тестов.

Следующее. Мы знаем, что вышел новый ГОСТ по безопасной разработке. Мы уже провели синхронизацию «Профиля защиты» (раздела 7.4) с требованиями данного теста. Провели анализ, выявили, что «Профиль защиты» не противоречит положениям ГОСТа, провели синхронизацию терминологий и постарались учесть недостающие моменты в «Профиле защиты».

Сейчас данная версия находится на внутреннем согласовании, надеемся, в начале года она выйдет в свет. Будем ждать уже дальнейшие разработки в продолжение ГОСТа, будем также проводить синхронизацию с ними, лучшие практики будем брать в наш «Профиль защиты» и адаптировать.

Ну и, конечно, ожидаем, что наш «Профиль защиты» всегда будет в «живом» и актуальном состоянии, надеемся на обратную связь рынка по этим положениям.

Спасибо большое за внимание. Я доклад закончил.

**Михаил Шабанов.** Спасибо, Константин.

Я надеюсь, что обновленный проект нового «Профиля защиты» вы пришлете в НАУФОР, и мы постараемся подключиться к обсуждению и внесению предложений.

А сейчас я хотел бы предоставить слово Андрею Киселеву. Тема его выступления звучит следующим образом: «Применение сертифицированного программного обеспечения: «потемкинская деревня» или реально выполнимое требование? Путь к безопасному процессу разработки».

Пожалуйста, Андрей, вам слово.

**Андрей Киселев**. Здравствуйте, коллеги!

Я бы хотел представить взгляд некредитной финансовой организации на процесс сертификации программного обеспечения, описать, как это выглядит со стороны регулируемой организации.

Немножко о нашей группе компаний. Это крупный регистратор, у нас больше 50 филиалов в стране, около 700 сотрудников, есть и депозитарная, и спецдепозитарная лицензия. В группу входит «НРК Фондовый рынок», которая, помимо депозитарной/ спецдепозитарной деятельности, имеет дилерскую деятельность. Поэтому мы должны обеспечивать стандартный уровень защиты.

В 2019 году руководство компании решило, что к различным сертификатам мы относимся положительно. Есть международный стандарт 27001, он обеспечивает безопасность в компаниях благодаря тому, что требует оценивать риски информационной безопасности, выстраивать процесс, постепенно улучшая безопасность. Мы пошли по этому пути, получили международный сертификат 27001, он нам очень помог пройти ГОСТ 57580.1. Получили достаточно

хорошую оценку, в общем, все достаточно хорошо.

Используем современные средства информационной безопасности, практически все отечественного производства. В следующем году будем менять «Чекпоинт». Он из дружественной страны, но его жизненный цикл заканчивается. Естественно, будем выбирать отечественного производителя.

Что хотел бы сказать? Я полагаю, что сертификация нужна Банку России для уверенности в том, что участники рынка используют защищенное программное обеспечение, и третья сторона это как бы подтверждала. Не просто участник рынка декларирует, что у него все хорошо, а третья сторона.

У нас в стране сертификацией занимается ФСТЭК, которая выдает сертификаты на средства защиты информации, ФСБ России (крипто средства), и Минобороны.

Хотел сказать пару слов о том, откуда взялся ГОСТ 15408. Вообще он родом из 70-х годов, это время зарождения основ информационной безопасности, Министерство обороны США в 1983 году выпустило «Оранжевую» книгу, параллельно ее адаптировали как раз в ГОСТ 15408, и вот так этот стандарт дошел до России.

По нашему ощущению, этот стандарт как бы нацелен на монолитные информационные архитектуры, которые в то время как раз и преобладали. Понятно, что Министерство обороны хотело себя каким-то образом обезопасить. Поэтому если кто-то хотел участвовать в тендере МО, предлагать свои разработки, то ему предлагали соответствовать ГОСТу 15408. Это обеспечивало уверенность, что система надежна и безопасна.

Понятно, что про сертифицированные средства говорится также и в 152 законе, и в 187-м.

Очень хорошо, что все-таки есть возможность перейти от сертификации к процессу безопасной разработки. Но в пункте 1.8 на самом деле предлагается только два варианта. Первый вариант — получить сертификат Федеральной службы по техническому и экспортному контролю. Эксперты писали, что пока таких сертификатов никто не получил. Это мертвый путь, никто им не идет.

Второй вариант — получить оценку соответствия по ОУД. Такую оценку можно, мы прорабатывали данный вопрос. Но насколько это полезно и нужно?

На мой взгляд, сертификация по ОУД-4 — это «потемкинская деревня». Не обязательно, конечно, за красивым фасадом будет разваленный дом, но он может там быть. Почему такая вероятность может реализоваться? Потому что, например, мы сертифицировали программное обеспечение и радуемся, что у нас есть соответствующая бумажка, всем ее показываем. Центробанк доволен, что мы сертифицировали. Но, например, при этом новые уязвимости валятся как из решета. Мы использовали какой-то компонент, он оказался очень уязвимым, его надо срочно закрывать. И возникает дилемма. С одной стороны, у компании есть бумажка, что программа безопасна. С другой стороны, реально безопасна программа будет, только если закрыть уязвимость. Что же делать? Нужно ли снова тратить много миллионов рублей и много часов времени, чтобы получить новую бумажку — либо подвергать клиентов опасности путем использования якобы защищенного программного обеспечения, которое по факту таким не является, но на которое есть бумажка?

Конечно, хорошо, что Банк России движется в сторону сертификации именно процесса, сюда и деньги не жалко вкладывать. Все мы хотим, чтобы у нас было защищенное программное обеспечение. Но есть «но».

«Но» представлено вот на этом слайде. Я знаю пять вендоров, которые предоставляют услуги по разработке программного обеспечения. Первый из них — это «Арка Технологии», ее надо выделить, потому что Владимир Курляндчик говорил, что они сертифицировались, получили оценку соответствия по ОУД-4 и это их выделяет среди других вендоров.

Что касается других вендоров… Поскольку я занимался по большей части регистраторской деятельностью, то мне ближе работа с вендором LDSoft. Они говорят: «Ребята, нас Центробанк обязывает сертифицировать программное обеспечение и процесс. А вас обязывает? Если хотите, сертифицируйте, мы всячески вам в этом поможем». В прошлом году мы пытались найти подрядчика, нам сказали, что полгода работы будут стоить 7 млн рублей. Честно говоря, у нас не так много денег, чтобы столько платить за соответствие. Есть гораздо более полезные вещи, которые будут повышать реальную безопасность: мы сейчас, например, с Wi №dows переходим на Astra Li №ux, и это далеко не бесплатно.

Тут напрашивается аналогия. Государство предлагает всем участникам процесса использовать электронную цифровую подпись. Называет вендоров, которые предоставляют услуги криптосредств. А ФСБ не заставляет вендоров сертифицировать средства защиты, но предложение сертифицировать получают физлица, причем за процедуру заплатит каждый. Вывод очевидный: такой механизм работать не будет.

Тех же регистраторов на рынке всего 31 штука, у некоторых прибыль составляет полмиллиона рублей, а за сертификацию надо заплатить 7 миллионов. Банк России тоже можно понять: мало ли какое ПО используют участники рынка. Как обеспечить уверенность в том, что софт надежный? Хотя рынок строился больше двадцати лет, вендоры конкурируют и сами заинтересованы в качестве своих продуктов. Например, компания LDSoft исполь-

зует защищенную базу данных, даже внутренние IT-специалисты не могли туда залезть. Это большое конкурентное преимущество.

В 90-х годах на рынке было много вендоров по регистраторской деятельности, были случаи, когда они использовали DBF базы, а их защитить очень тяжело. Был случай, когда какой-то системный администратор решил подзаработать, подправил в базе количество акций, вывел их на биржу, крутил там … в конце концов, это вылилось в скандал. Понятно, что это сильно ударило по конкретному вендору, рынок перестал использовать его продукты.

Что делать нашей компании? Допустим, у нас нет собственной разработки, есть только разработка внешних вендоров. Как мы можем сертифицировать не свою разработку? Я так понимаю, в предложенном Банком России пути есть только возможность сертифицировать именно свою разработку. Для крупных компаний, включая нас, это вариант. А для мелких — нет, они не смогут сертифицировать.

Выскажу предложение или пожелание. Почему бы Банку России самому не сертифицировать безопасные разработки существующих вендоров (их на рынке всего-то пять штук)? Я думаю, тот же LDSoft на это согласится: если ему не надо будет платить денег, он и документацию предоставит. Можно об этом поговорить. Мне кажется, и другие вендоры, тот же «Фэнси» и «Аванкор», пойдут навстречу Банку России. А Банк России сможет обеспечить рынку уверенность, что вендоры, работающие на финансовом рынке, разрабатывают безопасно. И между ними будет конкуренция. Все понимают, что выпущенные продукты этих вендоров безопасны. Рынок скажет большое спасибо. Я понимаю, что Банку России это тяжело сделать, но, может быть, все-таки какое-то решение возможно.

Ну и параллельно. Может быть, Банк России предоставит возможность, что

если подрядчик гарантирует безопасность своей разработки, что он соблюдает 57580.1, то можно будет сертифицировать все его продукты, а не только одну конкретную версию. Иначе мы получим ситуацию, когда невыгодно будет использовать системы автоматизации, и регистраторы перейдут на ручную работу. Бумажные документы будут принимать, а ЭЦП нет, потому что за использование ЭЦП могут получить штраф, а это очень дорого.

Тут есть разные возможности: независимый аудит кода, другие рыночные механизмы. Если мы понимаем, что LDSoft — это единственный вендор на регистраторском рынке, ну значит, он добился этого, можно проводить дополнительные аудиты его продукты, чтобы понять, что он разрабатывает безопасно.

Рынок был заинтересован в безопасной разработке, и за двадцать лет было добавлено очень много функций безопасности. Мне кажется, тут надо искать компромисс, потому что сейчас каждому НФО нужно вести «инхаус» свою разработку, а это ну очень дорого, рынок не потянет.

Коллеги, спасибо.

**Михаил Шабанов.** Андрей, большое спасибо за интересную презентацию.

Сейчас я хотел бы предоставить слово Евгению Цареву, управляющему RTM Group. Тем его выступления: «Подготовка к сертификации по безопасной разработке».

Евгений, пожалуйста, вам слово.

**Евгений Царев.** Коллеги, добрый день!

Меня попросили рассказать про безопасную разработку. Это очень важная история сейчас. Вдруг все узнали, что занимаются безопасной разработкой или занимались ей до этого всю свою жизнь, но только не знали, что это была безопасная разработка. Сейчас нужно заново договариваться о понятиях, о терминах, поскольку появился новый ГОСТ, который не учитывает сложившиеся по факту применения термины, которые имели хождение в среде специалистов. В общем, сегодня будем через это прорываться.

Следующий слайд.

Что важно сказать? Когда Центробанк начал заявлять, что рынок идет в сторону ОУД, это немножечко удивило, потому что к тому моменту все уже забыли про все эти критерии. По сути, ОУД был описан еще в какие-то лохматые годы, и непонятно, почему Центробанк прибегает к такой формулировке сейчас. Но что еще мог сделать Банк России? У Банка России есть задача повысить безопасность прикладного ПО, которое используется в коммерческих банках. Что регулятор может использовать в качестве нормативной базы? Да по сути, кроме ОУД, больше ничего. И когда появилась формулировка «оценочный уровень доверия», это сразу нас вернуло в гостехкомиссию, вернуло во ФСТЭК. Мы начали искать специалистов по тематике ОУД (почти все они уже вышли на пенсию), начали их звать к себе хотя бы для обучения персонала, хоть для какой-то помощи. Мы собрали определенную команду, которая позволила сформулировать услугу как таковую. И по состоянию на сегодняшний день у нас имеется значимое количество проектов. Сегодня будем об этом говорить.

Забегая вперед, мне вообще направление ОУД не очень нравится с точки зрения реальной безопасности. Коллеги про это частично говорили. Потому что проход по контролям, которые есть в ОУДах, существенно разрывается с реальной процедурной или процессной безопасностью.

Соответственно, мы сразу столкнулись с необходимостью выбора из двух опций: «шашечки» или ехать? Очень часто нужны именно «шашечки», нужно заключение о соответствии. И это, на мой взгляд, не очень рабочая история по той простой причине, что документы мы сделаем, конечно, и пройдем все этапы. Но если сразу же на этапе проверок специалисты перестанут делать какие-то процедурные вещи, то тут, собственно, всё. Поэтому вообще-то правильно идти от процессов.

Мы провели маленькое исследование, оценили, каково состояние уязвимостей в ПО тех заказчиков, с которыми мы работали. Мы ввели ряд понятий: «средний уровень опасности», «высокий уровень опасности», «критический уровень опасности» и «низкий уровень опасности». Это просто качественные оценки. Вывод приблизительно следующий: у тех, кто внедрял хотя бы отдельные элементы безопасной разработки, кто проводил хотя бы статический анализ, критичных уровней уязвимости мы не обнаруживали вообще. То есть даже элементарное внимание в направлении безопасной разработки дает результат сразу.

Это нас приводит к выводу, что безопасная разработка — это правильное приложение усилий (в данном случае, усилий субъектов контроля, то есть банков, страховых компании и так далее). И в какой-то момент после того, как появилось требование по ОУДу, стало очевидно, что ЦБ хочет заниматься безопасной разработкой и, по сути, стимулировать поднадзорных тоже заниматься безопасной разработкой. Это, в общем-то, правильно. Но как это обрамлять теперь, было не совсем понятно до появления ГОСТа, который вступит в силу с 20, что ли, декабря 2024 года.

Я думаю, в нормативную базу Центрального банка войдет и безопасная разработка. Мне кажется, что должен быть выбор: ты занимаешься либо ОУДом, либо безопасной разработкой. Фиксируешь либо одно, либо другое. Мы, наверное, к этому идем.

Но что показывает, опять же, практика? Она показывает, что если мы хотя бы на оценочном уровне понимаем, с чем

боремся и от чего пытаемся защититься, то это уже дает сумасшедший результат.

На следующем слайде вы видите изображение процесса безопасной разработки с встроенными механизмами, которые являются обязательными или необходимыми. Что отличает изображенный процесс от процесса обычной разработки? Мы видим, что анализ требований безопасности появляется на самом раннем этапе, уже на этапе планирования.

План тестирования безопасности — тоже интересная штука. Обычно разработчики (до появления, например, профессионального Security Champio №) подходят к этому этапу как к творческому. Они каждый раз делают новый план тестирования безопасности, это такая творческая история: вот мы сейчас внедряем что-то новое, а давайте будем в этом новом тестировать одно, а другое тестировать не будем.

Правила кодирования, контроль целостности, статический анализ, динамический фаззинг, ну и пентест готового приложения, которое появляется уже на этапе выпуска. Если все эти механизмы реализованы в организации хоть как-то, хоть как-то участвуют в процессе разработки, то это, на мой взгляд, радикально снижает вероятности даже сбоев. Как только тема безопасной разработки стала активно подниматься, появилось ощущение, что этим вопросом занялись больше с точки зрения экономии на поддержке. И, как показывает, опять же, практика, экономия на поддержке есть. Мне ее сложно оценить, но вот, допустим, в мобильных банковских приложениях радикально снижается нагрузка на техническую поддержку.

Распределение ролей в среде безопасной разработки большинство видит так: дизайнеры, разработчики, тестировщики делают основную работу, к ним надо подсоединить Security Champio N, фэнсив-инженера и так далее. В действительности, опять же, как показывает практика, часть этих ролей (может быть, за исключением Security Champio N) могут взять сами текущие разработчики. У нас есть направление с безопасной разработкой. И мы изначально закладывали, что там будут новые логики продукта, будут новые роли, новые люди в команде. А потом, когда началось закрытое тестирование, мы вдруг выяснили, что большинство тех, кто начинает пользоваться новым модулем, исполнение этих ролей возлагало на кого-то из существующей команды.

В общем, к чему я веду? Вдруг оказалось, что безопасная разработка дорого стоит. На встречах с представителями Банка России отечественные разработчики (большие компании, которые занимаются банковскими продуктами) говорили, что цена разработки вырастет кратно. Кто-то называл x2, кто-то — x7. Но вдруг выяснилось, что компоненты-то они стали внедрять, уже понимая, куда ветер дует, так что цена разработки сильно не увеличилась. Да, безусловно, она растет, но, скорее, растет больше от цены самих разработчиков и самих специалистов. То есть, если у компании в разработке трудится 50 человек, то сегодня они стоят, условно, 100 млн рублей, а через год они стоят уже 170 млн. От этого больше зависит.

Нормативное регулирование процедуры. Если вдруг кто-то не сталкивался с ГОСТом 56939, то вот с ним нужно, конечно, ознакомиться. И, на мой взгляд, мы будем отходить от концепции проверки программного продукта через направление анализа уязвимости или оценки соответствия по ОУДу. Приходить будем все-таки к процедурам безопасной разработки, это более логично. И я думаю, что если Банк России будет оставлять выбор (либо так, либо так), то многие пойдут в сторону именно безопасной разработки.

Что касается нормативного регулирования по ФСТЭКу, то здесь я, честно говоря, даже останавливаться не хочу. В нашей практике ни разу не было ни одной сертификации. Как только мы начинаем рассчитывать, сколько стоит эта цепочка в деньгах и во времени, вдруг все от нее отказываются. Поэтому даже говорить здесь ничего не будем. У нас из живых инструментов сегодня — ОУД, а завтра — ОУД плюс безопасная разработка.

Нормативное регулирование разработки безопасного программного обеспечения. На этапах разработки я тоже останавливаться особо не хочу. Мне все-таки хочется сказать, что даже если организация изначально, просто исходя из своих внутренних потребностей (снижения нагрузки на саппорт, повышение стабильности версий, снижение вероятностей отказа в работе) будет внедрять хотя бы часть из тех компонентов, которые здесь указаны, то этого достаточно. Это действительно очень сильно повышает безопасность программного продукта.

Опять же, по статистике, мы находили такое, что просто нельзя об этом даже говорить без применения к организациям. А продукты с точки зрения безопасности были небезопасны. Как только прошли первые проверки и пошли закрытия базовых вещей… Ну, чтобы вы понимали, как только приложение ставится в базе, у него технические пароли просто прописаны в поинте, и убрать их не получается. Какие-то безумные вещи. Вот как только часть компонентов внедряется, резко повышается безопасность ПО.

Могу обратить внимание на этап сборки ПО, это собственное наблюдение. На этапе сборки почему-то считается, что тот, кто будет делать сборку, сделает все правильно, ведь все компоненты прислали, что-то предварительно протестировали. А потом вдруг выясняется, что уже на этап эксплуатации попадают старые компоненты. Короче, по непонятной причине именно на этапе сборки (просто по наблюдениям) происходят странные телодвижения. Ну очень

странные вещи. Просто обратите внимание.

Хочется обратить внимание также на снижение рисков для бизнеса. Сейчас вопросы, связанные с утечками, переходят на какой-то новый уровень, и риски для бизнеса в этом плане возрастают, и внимание к этому со стороны государства возрастает. Оценка размер ущерба от утечки — тоже очень сложный вопрос.

В любом случае для бизнеса сегодня очень важно не попадать в исключительно бизнесовые проблемы. При этом проблем, связанных с недостатками программных продуктов, в том числе и в безопасности, такое ощущение, что становится больше. Раньше большинство инцидентов, которые мы наблюдали (процентов 80), было связано с банальными действиями сотрудников: зашел сисадмин в систему, воткнул жесткий диск, у него скопировалось все через «рейт», он диск вытащил и ушел с ним. Большинство инцидентов были такого типа.

Сейчас становится все больше инцидентов через уязвимости. И снижение рисков для бизнеса, наверное, сегодня является основным направлением. Необходимость реализации требований по безопасной разработки обосновывается относительно легко.

Вот предыдущий докладчик сказал, что очень странно платить за ОУД 7 миллионов. У нас были проекты и сильно дороже. А вот, например, потратить соизмеримые деньги на изменение или доработку процедуры, купить соответствующие программные продукты — это вроде, как и неплохо.

На этом закончу. Коллеги, если есть вопросы или комментарии, буду рад их услышать.

**Михаил Шабанов.** Евгений, большое спасибо.

Коллеги, пожалуйста.

**Александр Луганцев.** У меня будет один комментарий, если позволите. Вот как раз про отношения вендора и заказчика. Это не только касается ОУД-4. Получается два лагеря, по большому счету: с одной стороны, заказчики, с другой стороны, вендоры. В отношении ОУД-4 реализуется подход «проблемы негров шерифа не волнуют». Или «куда вы денетесь, все равно возьмете». И мы переходим к третьему этапу: нет у вас методов против Кости Сапрыкина. Я считаю, что это не совсем в данных условиях правильно.

**Михаил Шабанов.** Понятно. Спасибо, Александр.

Константин, у меня к вам вопрос, ну или, может быть, предложение. Вы как-то сможете откомментировать те нюансы, о которых говорили Андрей, Евгений, Александр?

**Константин Стародубов.** Да, безусловно. Банк России идет на то, чтобы заменить ОУД на безопасную разработку. Мы в связи с этим даже выпустили, повторяю, «Профиль защиты», в котором еще с 2022 года есть раздел 7.4, который регламентирует процесс безопасной разработки. То есть, когда компания часто выпускает релизы, то может сертифицировать процесс непосредственно безопасной разработки.

Но, к сожалению, там есть свои нюансы. ОУД-4 уже более обкатан на рынке, все уже знают, что с ним делать и куда бежать, а процесс безопасной разработки пока «темная лошадка», которая требует доработки. И сейчас мы хотим посмотреть на рынок, прежде чем внедрять его в качестве обязательного. Чтобы рынок посмотрел, как это внедряется, может быть, написал в Банк России запросы (мы их постараемся разъяснить), либо предложения по успешной имплементации тех мер и предложений, которые прописаны в 7.4. И когда мы наберем достаточно обширную статистику по тому, что профиль защиты работает (в частности, раздел 7.4, который регламентирует безопасную разработку), тогда посмотрим, как его можно внедрить непосредственно уже в Положение. Как внести ту развилку, которая позволит делать выбор: идти либо на ОУД, либо на безопасную разработку. Поэтому смотрим, наблюдаем. Пока Банк России дает участникам шанс попробовать внедрить, поэксплуатировать именно раздел 7.4, который, я напомню, планируется в ближайшее время синхронизировать с положениями ГОСТа.

**Михаил Шабанов.** Спасибо, Константин.

Но все-таки остался вопрос, касающийся работы с вендорами, которые предоставляют финансовому рынку программное обеспечение. Каким вы видите это направление работы? Потому что мы давно поднимаем этот вопрос, но он пока, как говорится, с мертвой точки не двигается.

**Константин Стародубов.** Пока у нас нет подтверждений, что хоть один вендор выполнил данное условие и сказал всем, что он соответствует разделу 7.4. Никто по этому пути не пошел. Ожидаем реакции и будем настаивать, что это допущение, а не обязательство.

**Михаил Шабанов.** Хорошо, я понял, что вопрос непростой, надо его каким-то образом совместными усилиями решать.

## III часть

**Импортозамещение: начало**

**Михаил Шабанов.** Мы переходим к финальной теме: «Импортозамещение». Открывает ее выступление Александра Плоткина, консультанта Центра координации обеспечения технологического суверенитета финансового рынка Департамента информационной безопасности Банка России. Тема выступления: «Импортозамещение: начало».

Александр, пожалуйста, вам слово.

**Александр Плоткин.** Коллеги, добрый день!

Сегодня поговорим об импортозамещении в кредитно-финансовой сфере. В рамках выступления затронем такие темы, как нормативно-правовое обеспечение нашей деятельности,

операционную деятельность и планы на будущее.

Начнем с нормативно-правовой базы. Сразу хочу оговориться, что действие не всех названных мной нормативных документов сейчас распространяется на всех участников, собравшихся здесь. Но подробнее пройдемся по каждому.

Сегодня поговорим о нормативном и правовом регулировании, взяв за точку отсчета Указы Президента №№ 166 и 250, весной 2022 года они были опубликованы. Это указы «О мерах по обеспечению технологической независимости и безопасности критической информационной структуры Российской Федерации», а также «О дополнительных мерах по обеспечению информационной безопасности».

В рамках реализации данных указов устанавливается запрет на использование иностранных средств защиты информации и программного обеспечения только для государственных организаций, а также формируется основание для введения запрета на использование иностранных программно-аппаратных комплексов. В частности, правительству поручается реализация соответствующих комплексных мероприятий.

Дополнительно стоит отметить, что в 250 Указе можно выделить дополнительные требования к структуре организаций в части обеспечения информационной безопасности, обязательному созданию соответствующих структурных подразделений и возложению на руководителя организации персональной ответственности за обеспечение информационной безопасности.

Как многие из вас помнят, Банк России уже весной 2022 года начал подготовку к реализации этих указов, мы проводили анализ имеющейся критичной архитектуры организаций в кредитно-финансовой сфере, в том числе некредитных организаций.

Одним из ключевых шагов в подготовке к реализации данных указов стало подписание в июне 2023 года 243 федерального закона, согласно которому Банк России был наделен полномочиями по контролю и мониторингу перехода финансовых организаций на преимущественное применение российского программного обеспечения и отечественного оборудования на значимых объектах КИИ, в том числе, в части согласования закупок на такие объекты.

Также данным федеральным законом была установлена обязанность некредитных финансовых организаций осуществлять переход на преимущественное использование российского ПО и оборудования на значимых объектах в соответствии с плановыми мероприятиями по переходу (согласованными с Банком России).

В свою очередь, правительством было выпущено несколько постановлений: Постановление № 1438 и № 1912.

Следующим этапом стала регистрация в мае 2024 года в Минюсте России Указания Банка России № 6679-У и 6680-У, которые устанавливали порядок проведения Банком России контроля и мониторинга за соблюдением реализации кредитными организациями и некредитными финансовыми организациями их планов мероприятий по переходу.

Стоит отметить, что на текущий момент контрольный срок перехода на значимых объектах — 1 января 2025 года для госорганизаций. Для субъектов КИИ, которые не имеют значимых объектов, а их достаточно много в рядах сегодняшних слушателей, Банк России проводит работу в рамках обеспечения операционной надежности и непрерывности оказания финансовых услуг.

В части нормативно-правового обеспечения мы рассмотрели все ключевые документы, касающиеся обеспечения техническуого суверенитета и импортозамещения, поэтому давайте перейдем к следующему слайду. На этом слайде описана операционная деятельность, которую проводил Банк России за последние два года: какие результаты получены, что будет дальше.

При определении наиболее критичных областей Банком России был проведен ряд мероприятий, в частности, оценка риска использования иностранных информационных технологий с точки зрения операционной надежности. Это Банк России проводил, в том числе, с некредитными финансовыми организациями и членами НАУФОР. В рамках данного мероприятия были ключевые этапы.

Первый этап: идентификация перечня используемых объектов информатизации критичной IT-архитектуры. Далее: оценка рисков операционной надежности по направлению обеспечения техсуверенитета, ну или импортозамещению. О ней мы поговорим чуть позднее. Третьим этапом стала подготовка планов перехода на российское программное обеспечение и оборудование, а также формирование основных направлений перехода.

Последний этап: непосредственно построение процесса непрерывного контроля и мониторинга в соответствии с полученными полномочиями, который на текущий момент в целом и реализуется.

Тут также стоит отметить, что все организации, которые с нами взаимодействовали по вопросу обеспечения суверенитета и импортозамещения, были поделены на две ключевые очереди. В первую попали те, у кого сроки жесткие (1 января 2025 года), во вторую очередь — все остальные. Сразу оговорюсь, что регулятор уделяет внимание всем организациям, но у тех или иных мероприятий могут быть сдвиги по времени в соответствии с нормативными документами.

На текущий момент Банк России осуществляет контроль и мониторинг планов перехода. Контроль и мониторинг осуществляются посредством форм отчетности по операционной надежности.

Рассмотрим чуть подробнее каждый из этапов. Процесс идентификации. Как это было? Процесс идентификации объектов информатизации осуществлялся с помощью разработанной Банком России функциональной технической карты (думаю, многие помнят, она была в формате Excel), она основана на типовых архитектурах финансовых организаций в нескольких разрезах (технологический процесс, бизнес-функции, автоматизированная система и объект информатизации). Этот процесс тесно связан с Положениями Банка России по операционной надежности (это № 779 и № 787).

Для более корректного и удобного предоставления информации от финансовых организаций Банк России разработал форму для заполнения, которая впоследствии одновременно стала и отражением текущего состояния финансовой организации с точки зрения операционной надежности.

В рамках работы по подготовке и реализации планов перехода было выделено три основных направления, по которым в Банке России существует рабочая группа и по которым организуется деятельность по реализации планов перехода.

Это, во-первых, программное обеспечение. Тут стоит выделить направление вендорского программного обеспечения и вертикально интегрированных платформ, а также области сервисов и аутсорсинговых услуг. В рамках второго направления деятельность ведется по отечественному оборудованию (аппаратное обеспечение и программно-аппаратные комплексы). Третьим направлением отдельно выделены средства защиты информации.

В части первого и второго направления, в том числе, ведется работа по формированию перечня доверенных программно-аппаратных комплексов на основании запросов от отрасли.

В рамках третьего направления определен состав решений и основных вендоров (разработчиков отраслевого ПО), ведется мониторинг осуществления перехода на эти вендорские решения, определены вертикально-интегрированные платформы, которые требуют изменения архитектуры при переходе, определена доля использования свободного программного обеспечения в IT-ландшафте финансовых организаций. Также ведется работа по систематизации внедрения цикла безопасной разработки. Об этом коллеги ранее уже говорили. Ну и, конечно же, внесение изменений в законодательство относительно использования аутсорсинговых услуг.

Теперь про оценку рисков. Оценка рисков выполнялась по методике, опять же, разработанной Банком России, включала в себя четыре основных направления. Третье направление: оценка риска превышения запаса прочности. Четвертое направление: информация о наличии риска нарушения сроков 166 Указа (но это опять же для тех, кому установлен срок перехода до 1 января 2025 года). Оценка мониторинга выполнения плана мероприятий для организаций, у которых установлены контрольные сроки, осуществляется на периодической основе.

Для контроля выполнения перехода на импортозамещенные решения организаций с госучастием Банк России выделил три ключевых этапа. Первый этап: подготовка планов. Далее процесс подготовки перехода в соответствии с установленными нормативами (Постановления Правительства № 1478 и № 1912). Третий этап: организация процесса мониторинга и контроля выполнения данных планов.

Для реализации координации обеспечения технологического суверенитета и импортозамещения финансового рынка было сделано следующее.

Получены правовые основания путем внесения изменений в соответствующий нормативный акт. Организовано взаимодействие с финансовыми организациями. Создана форма для сбора необходимой информации, в том числе, с использованием действующих источников. Обеспечена возможность оперативной обработки полученной информации. Построен процесс непрерывного контроля и мониторинга.

Теперь немножко поговорим о текущих и новых задачах, в рамках которых ведется работа и которые позволят развивать обеспечение техсуверенитета и импортозамещения кредитно-финансовой сферы в будущем.

В России проводятся Демо-дни, в рамках которых разработчики российского программного обеспечения презентуют свои проекты. Один из таких Демо-дней состоялся в сентябре в городе Сочи на XXI Международном банковском форуме «Финансовый рынок: технологический суверенитет и структурная трансформации экономики». Второй важный Демо-день запланирован на ежегодном Уральском форуме «Кибербезопасность в финансах». Указанные Демо-дни активно поддерживаются правительством и помогают развивать российские технологии.

Дальше хочется сказать, что в мае было опубликован перечень поручений Председателя правительства Михаила Владимировича Мишустина по итогам XXI Конференции цифровой индустрии, где одним из ключевых было поручение обеспечить подготовку методик оценки функциональной и технической зрелости отраслевых отечественных программных решений по сравнению с ведущими зарубежными аналогами, предложений по формированию типовых отраслевых стандартов и автоматизации производственных и управленческих процессов.

В кредитно-финансовой сфере оценка зрелости отраслевого программного обеспечения производится в соответствии со следующими приоритетами: первым приоритетом, конечно же, являются значимые объекты КИИ; на втором месте непосредственно операционная надежность; другие функции в рамках

бизнес-процессов организации стоят на третьем уровне, не приоритетном.

Соответственно, подход к определению готовности целевых решений, который мы предлагаем, включает четыре ключевых направления:

Первое направление: предоставление информации о выборе целевых решений в формате ФТК. Вторым этапом является предоставление информации о выбранных площадках, где планируется проводить тестирование (возможно, это будет организовывать сама компания либо отрасль).

Третий этап: завершение тестирования целевых прикладных решений, в Банк России предоставляется результат тестирования в формате анкеты, которую покажу чуть позднее. И четвертый этап: уже непосредственно оценка готовности отраслевых прикладных решений по методике.

На слайде вы можете увидеть пример заполненной анкеты в общем виде.

На этом у меня все. Спасибо большое за внимание.

**Михаил Шабанов.** Александр, большое спасибо.

Продолжим обсуждение следующим вопросом: «Регулирование и импортозамещение, исполнение указов президента». Слово предоставляется Вадиму Гриценко, начальнику Управления информационной безопасности ПАО «Московская биржа».

Вадим, пожалуйста, вам слово.

**Вадим Гриценко.** Добрый день, коллеги!

Продолжу выступление регулятора в том же ключе. Приятно видеть, что мы двигались в правильном направлении, в соответствии с тем, что только что проговорил Александр.

В группу Московской биржи входит организатор финансовой платформы маркетплейс «Финуслуги» и две системно значимые компании: «Национальный клиринговый центр» и «Национальный расчетный депозитарий». Соответственно, нашими клиентами являются как физические лица, так и профессиональные участники рынка ценных бумаг, клиенты, банки, разработчики ПО, федеральные органы исполнительной власти. В общем, клиент достаточно большой и разношерстный.

Я постарался скомпоновать на один слайд все те регуляторные требования, под которые мы подпадаем, которые должны были реализовать или сейчас в настоящее время реализуем.

Прежде всего, у нас как субъекта критической информационной инфраструктуры есть обязательства выполнения Указов президента №№ 250 и 166 для объектов КИИ, соответственно, до конца этого года мы должны заменить все средства защиты информации на российские.

При этом мы также должны реализовать требования для субъектов критической информационной инфраструктуры, перейти на отечественные СЗИ; мы попадаем под действие Приказов ФСТЭК № 239 и № 235 для значимых объектов критической информационной инфраструктуры, а в части перехода на российское ПО и оборудование, соответственно, должны реализовать требования Постановления правительства № 1912 и перейти на доверенный программно-аппаратный комплекс.

Вернусь к истории вообще проекта и программы импортозамещения. У нас в группе компаний значимыми объектами критической информационной инфраструктуры являются несколько систем, которые расположены в инфраструктуре наших компаний НРД и НКЦ. Проекты по импортозамещению этих технологий попали в проект № 163 «Импортозамещение технологий инфраструктуры» и в проект по импортозамещению прикладного ПО, СУБД и оборудования (проект № 212).

Вначале мы провели предпроект для значимых объектов критической информационной инфраструктуры, завершили его в прошлом году и плавно перетекли в реализацию проекта по реализации требований приказа ФСТЭК.

Все помнят 2022 год. Еще до выхода Указа президента у нас, так скажем, случилось событие системного риска: резко стали уходить иностранные компании, производители, вендоры программного обеспечения. Соответственно, снизилась отказоустойчивость, защищенность, все прекрасно помнят различные закладки в библиотеках программного обеспечения с различными лозунгами, или с отказом работы каких-то технологий и решений программного обеспечения.

Мы постарались, как говорил сейчас регулятор, провести оценку этих внезапно возникших рисков с учетом того, что по объективным причинам сыграл роль уход иностранных производителей, и возникла реальная необходимость перехода на новые технологии, на новое программное обеспечение. Это подкрепилось требованиями регуляторов, указами президента, необходимостью исполнения решений правительства в части импортозамещения. Также мы понимали, что для дальнейшего развития и реализации наших проектов потребуется резко перейти на отечественные решения или на те решения, которые, по крайней мере, не будут подвержены санкционному технологическому риску.

Мы провели оценку всех используемых у нас технологий, с учетом вероятности, так скажем, прекращения работы этих технологий, ухода вендора, отзыва лицензии, с учетом наличия на рынке аналогичных решений. Плюс оценили степень влияния перечисленных факторов на наши внутренние процессы, и с учетом критичности этого влияния определили три приоритета по реализации программы импортозамещения. Под одну из этих программ попали технологии обеспечения импортозамещения средств защиты информации.

Эти процессы, по требованиям указов президента, должны завершиться в текущем году. И, по большому счету, несмотря на определенные трудности

в начале пути, по большому счету, все иностранные решения уже заменены полностью или сейчас находятся в процессе импортозамещения.

С учетом того, что на российском рынке многие компании сейчас целятся к концу года успеть импортозаместиться, возникли сложности с поставками каких-то решений, лицензий и оборудования. Поэтому мы здесь иногда даже зависим не от себя, а от производителей. От вендоров, от поставщиков этих решений.

С учетом достаточно сжатых сроков (за полтора года необходимо было практически полностью трансформировать не только IT-ландшафт, но и ландшафт процессов обеспечения безопасности), мы считаем, что эти достаточно амбициозные планы мы все-таки успешно реализовали.

Кроме этого, в группе компаний Московской Биржи был реализован проект по обеспечению безопасности значимых объектов критической инфраструктуры. Как я ранее сказал, мы провели предпроект, пригласили стороннюю компанию и совместно с ней примерно оценили наши возможности и способности, как мы сможем перейти на отечественные технологии в области ЗКИ. К текущему моменту мы проект закончили, даже получили оценку, что соответствуем 187-ФЗ «О безопасности критичной инфраструктуры» и приказам ФСТЭК (на табличке я отобразил, сколько требований регуляторов мы в итоге успешно выполнили для того, чтобы получить позитивную оценку по соответствию требованиям законодательства по 187-ФЗ).

В рамках этих процессов мы утвердили структурные подразделения, которые отвечают за обеспечение безопасности объектов значимой инфраструктуры, дополнительно обучили персонал по программам повышения квалификации, утвердили проекты по системе безопасности СЗИ и, соответственно, внедрили сертифицированные средства защиты информации не ниже 5-го класса. Также

в группе компаний успешно внедряются процессы безопасной разработки, ну и, как я уже ранее сказал, идет импортозамещение средств и технологий защиты.

В дополнение к этому хочется сказать пару слов насчет замены программного обеспечения и других технологий, не относящихся к средствам защиты информации, для объектов критической информационной инфраструктуры. Московская Биржа совместно с ЦБ разработала планы по замещению этих технологий, у нас проходят регулярные встречи в ЦБ, мы отчитываемся, как выполняем требования регулятора по направлению замещения программного обеспечения, СУБД и технологий для значимых объектов критической инфраструктуры.

Также участвуем в других форматах. Есть такой Индустриальный центр компетенций «Финансы», в работе которого принимает участие Банк России, системообразующие компании финансового рынка, в том числе, Сбербанк, Т-Банк, банк ПСБ.

СПРАВКА. *В июне 2022 года правительство России поручило Минцифры совместно с рядом отраслевых федеральных министерств сформировать предложения по созданию в стране индустриальных центров компетенций (ИЦК). ИЦК представляет собой отраслевое сообщество крупнейших заказчиков, заинтересованных в замещении используемых программных продуктов и решений зарубежных вендоров на российские аналоги.*

Мы совместно с ИЦК «Финансы» прорабатываем тему импортозамещения, в том числе, разрабатываем методики тестирования средств и систем защиты. В частности, мы опрашивали всех участников ИЦК «Финансы», насколько российские решения, сейчас существующие на рынке, удовлетворяют требованиям заказчика по части надежности, производительности и так далее. Можно утверждать, что проблемы с надежностью, производительностью и стоимостью отечественных решений наблюдались, и, наверное, сейчас еще наблюдаются.

Московская биржа разработала отраслевой доклад на тему «Импортозамещение». В этом документе мы постарались обозначить существующие проблемы, систематизировать опыт отрасли. Также выделили основные проблемы и сложности на пути импортозамещения. Среди них, как я уже сказал, не совсем адекватная стоимость или не совсем удовлетворительное качество решений, которые представлены на нашем рынке, особенно на начальном этапе внедрения этих средств. Сейчас в рамках работы ИЦК «Финансы» мы проводим совместно с крупнейшими банками тестирование средств систем защиты. Надеемся, что наш опыт поможет компаниям при выборе адекватных средств систем защиты как раз таки при реализации этого сложного, но вместе с тем увлекательного пути.

Наверное, на этом все. Спасибо большое. Я постарался рассказать коротко. Если есть вопросы, задавайте.

**Михаил Шабанов.** Спасибо, Вадим. Пожалуйста, коллеги.

**Андрей Киселев.** Хочу задать злободневный вопрос? Вы систему идентификации относите к средствам защиты?

**Вадим Гриценко**. Мы сейчас, в рамках наших управляющих комитетов, которые определяют стратегию развития технологии, приняли решение использовать аутсорс-решения в качестве IDP провайдера от идентификации. Могу назвать, в принципе, «Кик-Лок». Он позволяет реализовать применение второго фактора для идентификации плюс дальше непосредственно саму систему идентификации можно использовать в качестве бэк-энда: например, доменную аутентификацию.

Плюс в качестве решения, которое обеспечивает непосредственно второй фактор, мы используем российское решение.

Это на самом деле достаточно сложный проект, потому что он должен охватить массу автоматизированных систем, информационных систем по части как раз аутентификации пользователей и управления пользовательскими учетными записями. И мы уже, наверное, второй год реализуем процесс внедрения нашего российского IDM. Изначально предполагалось внедрять решение иностранного производителя, но сейчас переходим на российский. И в целом, проект движется, хотя не без сложностей, безусловно.

**Михаил Шабанов.** Спасибо, Вадим.

Я хочу поблагодарить всех спикеров и экспертов, принявших участие в нашей конференции. Надеюсь, что выступления были интересными и полезными, что они будут использованы нашими слушателями, в том числе в вопросах, связанных с обеспечением информационной безопасности.

Спасибо всем за внимание. ◻