

---

**Михаил Шабанов**

председатель комитета НАУФОР по экономической  
и информационной безопасности

# Обязательства по защите

**В эпоху цифровизации риски информационной безопасности являются важнейшей составляющей операционного риска**

Михаил Шабанов, председатель комитета НАУФОР по экономической и информационной безопасности, рассказывает журналу «Вестник НАУФОР» о проблемах и парадоксах отрасли информационной безопасности, а также предлагает алгоритмы решений.

Фотографии **Сергей Ермохин**

— Какие основные тенденции вы видите в нормативных изменениях по вопросам информационной безопасности в части НФО (НКО)?

— Прежде всего, я бы хотел отметить, что до 2019 года, до момента принятия Банком России Положения № 684-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», большинство требований стандартов, связанных с обеспечением информационной безопасности в некредитных финансовых организациях (НФО), носили рекомендательный характер. Так что мо-

ментом, с которого у НФО возникают обязательные требования по обеспечению информационной безопасности и необходимость их исполнения, считается 2019 год.

Да, эпидемия COVID-19 внесла существенные изменения в сроки реализации отдельных требований Положения № 684-П (ныне отменённого), также это касается требований нового Положения 757-П (см. Информационные письма от 2020–2021 годов). По сути, сроки реализации распространяются до конца текущего года, а далее некредитные финансовые организации обязаны продемонстрировать надзорному органу в лице Банка России их соответствующее исполнение. В эпоху сплошной цифровизации риски информационной безопас-

ности являются, по сути, важнейшей составляющей операционного риска. Они требуют пристального внимания со стороны НФО по следующим причинам:

- регулирование этих вопросов в некредитных финансовых организациях-участниках фондового рынка имеет сравнительно недавнюю историю; в том числе, отсутствует статистика по оценке влияния регулирования на снижения киберрисков и рисков мошенничества;
- количественная оценка уровня риска для конкретной НФО и формирования резерва под возможные потери являются сложными задачами;
- факторы, влияющие на уязвимость процессов и технологий НФО, постоянно изменяются; это значит, что потенциально они могут влиять на активы НФО по направлениям: репутация, конфиденциальность, целостность, доступность, авторизованность операций;
- проблемы как мировой, так и российской (плюс страны СНГ) экономики опосредованно повышают мотивацию потенциальных злоумышленников, как внешних, так и внутренних: в период ухудшения экономической ситуации может наблюдаться тенденция к росту правонарушений.

С момента передачи (в 2018 году) Банку России права определять для поднадзорных организаций политику в области обеспечения информационной безопасности произошли серьезные изменения, которые в полной мере затронули деятельность профессиональных участников рынка ценных бумаг.

В качестве основных задач в области информационной безопасности и киберустойчивости Банком России были определены:

- 1) обеспечение киберустойчивости;

- 2) защита прав потребителей финансовых услуг через мониторинг показателей уровня финансовых потерь;

- 3) содействие развитию инновационных финансовых технологий в части контроля показателей риска реализации информационных угроз и обеспечение необходимого уровня информационной безопасности.

Реализация этих задач включает в себя и такую составляющую, как разработка и утверждение нормативно-правовых актов, распространяющихся на большинство некредитных финансовых организаций.

### В эпоху сплошной цифровизации риски информационной безопасности являются, по сути, важнейшей составляющей операционного риска.

— Какие элементы этого регулирования сегодня становятся объектом внимания регулятора или источником проблем участников рынка?

— В теории обеспечения информационной безопасности все достаточно просто и понятно. За многие годы в мире наработан большой опыт по защите информации. Существует множество международных и отечественных стандартов.

Но на практике у некредитных финансовых организаций возникает множество вопросов, на которые, в отсутствие квалифицированных специалистов внутри самой компании, трудно получить правильные ответы.

Прежде всего, НФО должны были провести самооценку состояния информационной безопасности в компании, а затем подготовить программу действий, направленную на реализацию требований Положения. При этом необходимо учитывать требования в области обеспечения информационной безопасности,

связанные с исполнением Федерального законодательства (152-ФЗ «О персональных данных», 187-ФЗ «О безопасности критической информационной инфраструктуры», 63-ФЗ «Об электронной подписи») и требований нормативно-правовых актов ФСТЭК, ФСБ и Мнкомсвязи.

Также необходимо учесть проекты документов, готовящиеся Банком России в области защиты информации в некредитных финансовых организациях (главным образом, проект Положения «Об установлении обязательных для некредитных финансовых организаций

требований к операционной надежности при осуществлении деятельности в сфере финансовых рынков в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)». А также проект национального стандарта Российской Федерации ГОСТ Р «Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер».

— Каковы нынче основные проблемы и тенденции в области обеспечения информационной безопасности для некредитных финансовых организаций?

— Перечислю основные проблемы. Во-первых, имеет место дефицит специалистов, способных грамотно, а главное, в практической плоскости ориентироваться во всех созданных в этой области документах, классификаторах, ГОСТах и категориях всех уровней существующих документов. Это несложная задача,



если задаться такой целью. Однако, разбираться только в этом недостаточно для построения комплексной системы обеспечения информационной безопасности.

Далее, налицо дефицит специалистов, способных самостоятельно определить уровень необходимости и достаточности применяемых организационных и технических мер по информационной безопасности в компаниях кредитно-финансовой сферы. Невысок уровень понимания неотвратимости развития контроля над состоянием информационной безопасности со стороны государства, надзорных органов, включая Банк России.

Недостаточен уровень понимания серьезности и опасности уже существующих угроз, в том числе для собственников бизнеса НФО. Мало кто оценивает наличие и вероятность реализации угроз на основании не информации в СМИ, а собственных мер по анализу своих реальных условий и уязвимостей ИБ. Недостаточен поэтому и уровень понимания неотвратимости затрат по направлениям, связанным с обеспечением информационной безопасности в дальнейшем. Стремление сэкономить будет приводить к нарушениям, а, возможно, и хуже — к потерям. А оптимизировать расходы по информационной безопасности люди пока не научились.

Важно отметить, что любые попытки организовать массовую системную помощь со стороны для исполнения требований регулятора в области обеспечения информационной безопасности в НФО будут мало эффективны в плане достижения желаемого результата.

— Почему?

— Слишком разнообразны организационные структуры, индивидуальные подходы в ведении бизнеса, есть множество неочевидных тонкостей. Регулятор

также не стремится довести требования до «запятой и буквы», предоставляя исполнителю определенную степень свободы в организации решения поставленных задач. Реальная помощь может быть только индивидуальной. Никаким универсальным пакетом документов (например, для НФО) не поможешь, в любом случае потребуются значительные финансовые и человеческие ресурсы для реализации требований Положения № 757-П, ГОСТов, Федеральных законов.

— Насколько компании сегодня в целом защищены, как вы оцениваете этот уровень?  
— В настоящий момент еще не вступил

**Недостаточен... уровень понимания неотвратимости затрат по направлениям, связанным с обеспечением информационной безопасности в дальнейшем. Стремление сэкономить будет приводить к нарушениям, а, возможно, и хуже — к потерям.**

в силу ряд требований Положения 757-П, относящихся к проведению проверки соответствия определенного уровня обеспечения защиты информации требованиям ГОСТ 57580.1-2017, а это означает, что объективная информация по данному вопросу отсутствует. Однако в октябре 2020 года по инициативе комитета по экономической и информационной безопасности был проведен опрос членов НАУФОР в целях анализа текущих проблем экономической и информационной безопасности, существующих в некредитных финансовых организациях.

Его результаты (с определенными оговорками) выглядят следующим образом.

■ В ответах не были отражены успешные целевые атаки на критично важные активы компаний. То есть, целевых атак, которые бы позволили злоумышленникам преодолеть защиту и закрепиться в инфраструктуре НФО

для целей кражи данных и/или несанкционированных операций, выявлено не было;

- Респонденты выделили в сегменте информационной безопасности инциденты, информация о которых была своевременно направлена в ФинЦерт Банка России. Однако следует отметить, что инциденты ИБ не привели к финансовым потерям и не нанесли ущерб компаниям;
- 100 % респондентов отмечают, что руководство осознает важность обеспечения информационной безопасности;
- У 16 % компаний есть выделенное подразделение, у 31 % — выделенные

сотрудники. Остальные 53 процента НФО обеспечивают информационную безопасность посредством распределения обязанностей, которые могут возлагаться как на генерального директора, так и на иных сотрудников по совмещению;

- Достаточность бюджетирования подтвердили 75% респондентов;
- 52 % опрошенных отметили наличие трудностей с внедрением Положения №684-П — в первую очередь, в связи с требованиями по анализу уязвимостей прикладного ПО и приложений по ОУД-4;
- Те 48% респондентов, которые ответили, что трудностей с внедрением нет, дополнительно прокомментировали, что уровень риска, возникающий из-за наличия уязвимости в ПО и объем средств, затраченных на

оценку уязвимостей по ОУД-4, не позволяет говорить об экономической эффективности данного требования;

- 27 % респондентов ответили, что для обеспечения информационной безопасности компании пользуются внешними сервисами.

Результаты опроса позволяют сделать определённые выводы. Экстраполируя общий уровень информационной безопасности, реализованный в системах компаний-членов НАУФОР, состояние информационной безопасности в целом по отрасли можно считать удовлетворительным. Риски информационной безопасности, присущие кредитно-финансовой сфере (целевые атаки), имеют низкую вероятность существенно повлиять на российский рынок ценных бумаг; процессы и технологии защиты, в целом, адекватны. Между тем, результаты обзора показывают, что в большинстве НФО (53%) отсутствует специальное подразделение и сотрудники, занимающиеся вопросами обеспечения информационной безопасности. Это будет являться большой проблемой при реализации требований Положения № 757-П.

— **Насколько усиление дистанционного взаимодействия повысило актуальность ужесточения требований к информационной безопасности?**

— Переход большинства компаний финансового рынка во время пандемии на «удаленку» безусловно повысил актуальность задач по обеспечению информационной безопасности. Прежде всего — при осуществлении удаленного доступа с использованием мобильных/переносных устройств.

Отдельного ужесточения требований со стороны надзорных органов, включая Банк России, не было. Но многие сотрудники НФО почувствовали необходимость выполнения определенных требований и наличия

определенных знаний в области защиты информации для исполнения своих служебных обязанностей вне офисных помещений.

— **Как выстраиваются подходы к вопросам информбезопасности в крупных и мелкие компаниях; различаются ли они; насколько сегодня актуальна самостоятельная разработка защиты?**

— Большинство крупных и средних компаний финансового рынка так или иначе входят в экосистему определенных финансовых (банковских) холдингов, что существенно меняет их подход к реализации требований Положения 757-П по сравнению с компаниями малого бизнеса. Прежде всего, отметим, что финансовые холдинги двигаются в сторону создания такой инфраструктуры ИБ, которая позволила бы им закрыть все вопросы.

Речь идет о создании внутри холдинга компаний, имеющих необходимые лицензии ФСТЭК и ФСБ для проведения необходимых работ по требованиям Положения №757-П, о привлечении в компании высококвалифицированных специалистов в области обеспечения ИБ, а также о закупке необходимых программно-аппаратных средств по защите информации.

В небольших компаниях намечается совсем другая тенденция: они привлекают сторонние компании — интеграторов информационной безопасности для того, чтобы закрыть все вопросы исполнения требований по защите информации.

Нужно только отметить, что ответственность в любом случае остается на НФО, которая и будет отвечать за разработку, утверждение и контроль исполнения соответствующих организационных и технических мер информационной безопасности.

— **Какие принципиальные новации содержит Положение № 757-П Банка России?**

**Насколько удалось в дискуссии с регулятором изменить те или иные позиции?**

— Хотелось бы отметить что, начиная с выхода Положения №684-П, мы находились в постоянном контакте с представителями Департамента информационной безопасности Банка России и неоднократно направляли вопросы и предложения по совершенствованию данного Положения.

Часть наших предложений была учтена, по некоторым вопросам был найден компромисс, а где-то нам не удалось отстоять нашу точку зрения. (Например, в новом Положении мы увидели раздел, посвященный требованиям обеспечения минимального уровня защиты информации).

Итак, 20 апреля 2021 года Банк России опубликовал на своем сайте проект Положения № 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».

Документ полностью изменил свою структуру, теперь он состоит из 4 глав. И если 1 и 4 главы практически идентичны тексту Положения №684-П, то 2 и 3 главы являются нововведением для некредитных финансовых организаций.

Одним из ключевых изменений, которое бросается в глаза уже при первом прочтении документа, является изменение перечня некредитных финансовых организаций, реализующих усиленный и стандартный уровни защиты информации; а также выделение перечня некредитных финансовых организаций, которые реализуют минимальный уровень защиты информации.

Также немаловажно выделение Банком России особенностей обеспечения защиты информации для операторов

ра финансовой платформы, регистратора финансовых транзакций (Глава 2) и оператора информационной системы, в которых осуществляется выпуск цифровых финансовых активов, оператора обмена цифровых финансовых активов (Глава 3).

— **Насколько усложнилась сдача ПО в аренду?**

— Если разработчик ПО собственными силами или с привлечением сторонней организации проводит проверку по ОУД 4, то никаких проблем с использованием прикладного ПО и приложений не возникает.

Необходимо отметить, что требования Положения 757-П распространяются на некредитные финансовые организации и не применимы для компаний разработчиков ПО; в случае, когда работа не проводится, арендатору ПО придется самостоятельно проводить проверку ПО по ОУД-4, а для этого потребуются предоставить разработчику большой объем информации, включая исходный код сдающегося в аренду ПО.

— **Каковы рекомендации со стороны НАУФОР по выбору компаний, способных обеспечить для компании-НКО информационную безопасность?**

— НАУФОР — саморегулируемая организация, не занимающаяся коммерческой деятельностью, и мы не вправе продвигать те или иные компании, занимающиеся предоставлением сервисов или услуг в области информационной безопасности. Вместе с тем, мы используем комитет как платформу для знакомства членов НАУФОР с компаниями — интеграторами программно-аппаратных средств и сервисов информационной безопасности. С начала года мы провели три таких расширенных заседания нашего комитета, на которые приглашали всех желающих членов НАУФОР.

Планируем продолжить эту работу.

— **Будет ли НАУФОР разрабатывать собственные стандарты (или типовые внутренние документы) по защите информации?**

**Насколько, по вашему мнению, компании погружены в проблематику, требуются ли им дополнительные разъяснения?**

— В июле 2020 года по инициативе НАУФОР была проведена встреча с руководством Департамента информационной безопасности Банка России по поводу выполнения требований Положения 684-П. Там была озвучена отрицательная позиция регулятора относительно разработки саморегулируемыми организациями специальных стандартов в области обеспечения ИБ.

Вместе с тем, после выхода нового Положения комитетом была создана рабочая группа по разработке типовых

внутренних документов по защите информации для некредитных финансовых организаций. Надеюсь, что к концу года у нас появятся первые результаты и мы ознакомим с ними всех заинтересованных членов НАУФОР.

Но хочу обратить ваше внимание, что это документы верхнего уровня, без глубокой детализации. Как вы прекрасно понимаете, бизнес-процессы, например, в брокерской компании и в управляющей компании существенно различаются. Сделать документы, которые могут всем подойти, мы можем только на верхнем уровне.

— **Как вы оцениваете работу системы сертификации? Что нужно в ней поправить?**

— Исходя из нашего общения с разработчиками программного обеспечения

и приложений для проведения финансовых операций в НФО, можно сделать следующий вывод. Сертификация одного ПО в системе ФСТЭК в среднем может продолжаться до двух лет.

В условиях, когда в течение года компании-разработчики предоставляют несколько версий и десятки обновлений, сертификация безнадежно устаревает. Вывод: сертификация ПО такого класса фактически невозможна (к моменту сертификации ПО безнадежно устаревает). Речь может идти только о проверке ОУД-4.

— **Требуется ли сертифицировать программное обеспечение сайта компании, содержащее личный кабинет клиента? В каких случаях?**

**Мы используем комитет как платформу для знакомства членов НАУФОР с компаниями — интеграторами программно-аппаратных средств и сервисов информационной безопасности. С начала года мы провели три таких расширенных заседания.**

— Как я уже отметил, сертификация в нашем случае — не лучший вариант. Кроме того, необходимо учитывать, какой уровень защиты информации необходимо обеспечивать НФО.

Например, если речь идет о минимальном уровне защиты информации, то компания вправе самостоятельно решить вопрос о необходимости проведения сертификации используемого ПО в системе ФСТЭК или проведение его анализа по ОУД-4. А о каких случаях идет речь, не скажешь лучше, чем это прописано в пункте 1.8 Положения № 757-П. Цитирую, выделив наиболее важное. «Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечить использо-







вание для осуществления финансовых операций прикладного программного обеспечения автоматизированных систем и приложений, распространяемых некредитной финансовой организацией своим клиентам для совершения действий в целях осуществления финансовых операций, а также программного обеспечения, обрабатывающего защищаемую информацию при приеме электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием информационно телекоммуникационной сети «Интернет», сертифицированных в системе сертификации Федеральной службы по техническому и экспортно-

му контролю на соответствие требованиям по безопасности информации, в том числе на наличие уязвимостей или недекларированных возможностей, или в отношении которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия не ниже, чем ОУД-4, предусмотренного пунктом 7.6 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013.

Некредитные финансовые организации, не реализующие усиленный и стандартный уровни защиты информации, должны самостоятельно определять необходимость сертификации или оценки соответствия прикладного программ-

ного обеспечения автоматизированных систем и приложений.

В отношении программного обеспечения и приложений, не указанных в абзаце первом настоящего пункта, некредитные финансовые организации должны самостоятельно определять необходимость сертификации или оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений».

— Создает ли передача функций на аутсорсинг (например, от управляющей компании к спецдепозитарию) дополнительную нагрузку на систему безопасности?

— В связи с тем, что для НФО не принят специальный нормативный документ в



этой области, я предлагаю ориентироваться на Стандарт, разработанный Банком России (для банковской системы) СТО БР ИББС-1.4-2018 «УПРАВЛЕНИЕ РИСКОМ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ АУТСОРСИНГЕ».

В качестве ремарки в данном стандарте отмечается, что «передача выполнения бизнес-функций на аутсорсинг не снимает обязанности и не переносит ответственности организаций БС РФ, включая вопросы обеспечения ИБ, предусмотренные законодательством РФ, в том числе нормативно-правовыми актами РФ, нормативными актами Банка России.

— Зависят ли подходы к безопасности от вида деятельности (например, у профучастника и УК)?

— Безусловно, различия существуют, но в большей степени это относится к бизнес-процессам и тем критериям, которые прописаны в Положении 757-П для определения, какой уровень информационной безопасности необходимо обеспечить НФО.

— Есть ли в этом плане особенности у компании, которая делает витрину или маркетплейс?

— Если мы ведём речь о маркетплейсах (по сути, они являются финансовой платформой, где регистрируются финансовые транзакции), то оператору этих платформ, дополнительно к мерам по защите информации, указанным в Главе 1 в пункте 1.1 Положения 757-П, необходимо осуществлять защиту информации в соответствии с требованиями, прописанными в Главе 2.

— Можно ли разделить внутри одной организации контуры, которые будут защищены по стандартному и по минимальному уровню?

— Безусловно, можно. Но для этого вы должны провести соответствующий аудит всех программно-аппаратных средств, сетевого оборудования, используемого программного обеспечения для осуществления бизнеса в вашей некредитной финансовой организации, разобравшись со всей совокупностью объектов

информатизации. Далее надо будет в соответствии с определённым ранее необходимым уровнем обеспечения информационной безопасности выделить контуры безопасности с единой степенью критичности и единой политикой защиты информации. А на следующем шаге — соответствующим образом защитить.

— Требуется ли использовать усиленную подпись (с криптографией) во всех случаях? когда допустимо использовать простое подтверждение (смс и пароль)?

Сегодня нет необходимого соотношения между реальными существующими рисками ИБ в кредитно-финансовой сфере и количеством специалистов, которые готовы эти риски выявлять и успешно закрывать.

— Если вашей некредитной финансовой организации необходимо обеспечивать усиленный или стандартный уровни защиты информации, то необходимо обеспечивать использование усиленной электронной подписи или иных СКЗИ, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения.

За одним исключением. Если передача электронных сообщений происходит по выделенным информационно-вычислительным сетям, а НФО предоставляет заключение об неактуальности выделенных угроз, то можно не исполнять это требование.

Если обратится к компаниям, которым необходимо обеспечить минимальный уровень защиты информации (п.1.4.4 Положения 757-П), то необходимо обратиться к соответствующим положениям ГОСТа 57580.1-2017 и проверить, насколько используемый в вашей компании метод идентификации, аутентификации и авторизации соответствует ГОСТу.

Если под смс и паролём мы понимаем двухфакторную модель аутенти-

фикации, то это в полной мере соответствует минимальным требованиям ГОСТа. Также можно для этих целей использовать обычную, однофакторную модель аутентификации. Но лучше сопоставить все детали и сделать необходимые выводы.

— Каково состояние кадрового состава специалистов по информационной безопасности, достаточно ли на рынке квалифицированных специалистов?

— К большому сожалению, после 2019 года (с момента возникновения соответ-

ствующих требований в области защиты информации в НФО) на рынке возник дефицит квалифицированных специалистов в этой области. Парадокс бурно развивающейся отрасли информационной безопасности состоит в том, что для успешного обучения специалистов в вузах и для их дальнейшей востребованности необходимо готовить такие учебные программы, которые будут актуальны не сейчас, а в перспективе. Сегодня нет необходимого соотношения между реальными существующими рисками ИБ в кредитно-финансовой сфере и количеством специалистов, которые готовы эти риски выявлять и успешно закрывать. Выпускники вузов зачастую обучаются тому, что к моменту их трудоустройства становится мало актуальным. Кроме того, специалист ИБ должен понимать не только и не столько, как работает безопасность. Он должен понимать, как работает основной бизнес и что этот бизнес может потерять, если будет неправильно построена комплексная система обеспечения безопасности в компании. Помимо устаревших про-

грамм, еще одна проблема. Она состоит в неготовности некоторых руководителей финансовых организаций понимать, что нужен именно специалист, понимающий технологии и бизнес компании. По имеющейся информации, в перспективе Банк России намерен эту проблему решать путем постепенного введения в обязанность для любой финансовой организации иметь в штате специалиста, прошедшего определенное обучение в области обеспечения ИБ.

Кроме того, Банк России планирует вводить аттестацию специалистов по информационной безопасности, подтверждающую их квалификацию, но только после того, как появятся профессиональный и образовательный стандарты и будут запущены учебные программы в нескольких вузах, произойдут изменения в нормативной базе.

В 2020 году по инициативе Банка России и Совета по профессиональным стандартам финансового рынка я возглавил рабочую группу по разработке профессионального стандарта «Специалист по информационной безопасности в кредитно-финансовой сфере». COVID-19 внес в эту работу определенные сдвиги по времени, но я рад сообщить, что в настоящее время проект профстандарта находится на согласовании Минтруда.

Надеюсь, что до октября мы получим заключение и выйдем на завершающую стадию его подписания.

— Коснулась ли этой деятельности реформа оценки квалификации, насколько оценка квалификации эффективна сегодня в отношении таких специальностей?

— Поскольку в настоящее время профессиональный стандарт отсутствует, то и независимые центры оценки квалификации специалистов по информационной безопасности в кредитно-финансовой сфере не создавались.

Существует инициатива комитета НАУФОР о возможности включения вопросов обеспечения ИБ в нефинансовой организации в квалификационные вопросы, при проведении независимой

оценки профессиональных специалистов рынка ценных бумаг.

— Если в штате организации нет специалиста по информационной безопасности, то какие именно организационные меры должна она самостоятельно разрабатывать?

Отсутствие специалистов по информационной безопасности в компании никаким образом не освобождает от исполнения требований федеральных законов, нормативно-правовых актов и, прежде всего, нормативных документов Банка России в области защиты информации. Какие именно при этом необходимо использовать организационные и технические меры, зависит от того, какой уровень защиты информации (усиленный, стандартный или минимальный) в компании будет обеспечиваться.

— Как вы оцениваете уровень диалога с Банком России и сертифицирующими органами?

— Могу отметить, что с момента создания в 2018 году комитета по экономической и информационной безопасности НАУФОР у нас сложились рабочие отношения со специалистами Банка России — прежде всего, с сотрудниками Департамента информационной безопасности.

— Какие задачи сейчас стоят перед комитетом НАУФОР по экономической и информационной безопасности?

— С момента утверждения в 2017 году Советом директоров НАУФОР Положения о комитете его цели и задачи не изменились. Однако с 2019 года комитет существенно больше внимания стал уделять вопросам информационной безопасности, принимая активное участие в обсуждении проектов нормативных документов, подготавливаемых Банком России.

Комитет продолжает активно взаимодействовать с различными общественными организациями — такими, как Аналитический центр «Форум», Ассоциация по экономической безопасности «Звезда», Академия информационной безопасности Сбера и Ассоциация ФИНТЕХ. Представители комитета участвуют в работе в подгруппе 14 «Информационная безопас-

ность» по устранению устаревших и избыточных регуляторных требований в нормативных актах по вопросам, относящимся к компетенции Банка России и в работе Технического комитета № 122 «Стандарты финансовых операций» по разработке и принятию национальных стандартов в области защиты информации. На заседаниях комитета регулярно рассматриваются вопросы, связанные с реализацией требований Положения Банка России «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», по разработке профессиональных стандартов для специалистов в области финансовых технологий и специалистов по информационной безопасности в кредитно-финансовой сфере.

Комитет является организатором работы по проведению семинаров с участием IT-компаний, занимающихся разработкой и внедрением программно-аппаратного и программного обеспечения по вопросам создания, мониторинга и совершенствования комплексной системы информационной и/или экономической безопасности в некредитных финансовых организациях. И на сегодня с начала года мы провели уже три расширенных заседания комитета, на которые были приглашены все желающие — члены НАУФОР. Не прекращаем заниматься работой по противодействию сайтам, распространяющим заведомо ложную информацию, порочащую деловую репутацию участников российского рынка ценных бумаг, а также по выявлению и блокировке фишинговых сайтов, маскирующихся под вид сайтов компаний, оказывающих услуги на российском рынке ценных бумаг и распространяющих вредоносные программы. □