Бурцев Сергей Ильич, магистрант,
Сургутский государственный университет
г. Сургут

Макаренко Илья Викторович, магистрант,
Сургутский государственный университет,
г. Сургут

ВОПРОСЫ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ КОРПОРАТИВНОГО УПРАВЛЕНИЯ ПРОФЕССИОНАЛЬНЫХ УЧАСТНИКОВ РЫНКА ЦЕННЫХ БУМАГ

Аннотация: эффективное управление рисками информационной безопасности в рамках осуществления внутреннего контроля является важной составляющей развития в Российской Федерации устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных. Профессиональные участники являются непосредственными участниками этого масштабного процесса, так как должны соответствовать высочайшим стандартам информационной безопасности в процессе осуществления операций на рынке ценных бумаг. Должностные лица, осуществляющие управление рисками информационной безопасности в профессиональных участниках, выполняют важную институциональную роль по внедрению в организациях новых отечественных технологий и лучших международных практик и стандартов внутреннего контроля и аудита соответствии с требованиями законодательства Российской Федерации.

Ключевые слова: цифровая трансформация, риски информационной безопасности, критическая информационная инфраструктура, операционный риск.

В настоящее время вопрос разработки отечественного программного обеспечения (далее – ПО) стал одним из приоритетных в государственной политике Российской Федерации. Цифровая трансформация отнесена к национальным целям Российской Федерации. В частности, в п.8 Указа Президента РФ от 07.05.2024 №309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» следующие цели были определены как национальные цели развития Российской Федерации на период до 2030 года и на перспективу до 2036 года:

- цель обеспечения в 2025 – 2030 годах темпов роста инвестиций в отечественные решения в сфере информационных технологий вдвое выше темпа роста валового внутреннего продукта
- переход к 2030 году не менее 80 процентов российских организаций ключевых отраслей экономики на использование базового и прикладного российского программного обеспечения в системах, обеспечивающих основные производственные и управленческие процессы;
- увеличение к 2030 году до 95 процентов доли использования российского программного обеспечения в государственных органах, государственных корпорациях, государственных компаниях и хозяйственных обществах, в уставном капитале которых доля участия Российской Федерации в совокупности превышает 50 процентов, а также в их аффилированных юридических лицах.

Следует отметить, что уже в 2018 году п.11 Указа Президента РФ от 07.05.2018 №204 (ред. от 21.07.2020) «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» предписывал Правительству Российской Федерации при

реализации совместно с органами государственной власти субъектов Российской Федерации национальной программы "Цифровая экономика Российской Федерации" обеспечить в 2024 году достижение целей по:

- созданию устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств;
- использованию преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления и организациями;
- обеспечению информационной безопасности на основе отечественных разработок при передаче, обработке и хранении данных, гарантирующей защиту интересов личности, бизнеса и государства.

Для реализации поставленных задач в марте 2022 года указом Президента РФ от 30.03.2022 №166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» (далее – Указ №166) были введены ограничения на использование иностранного ПО, которые коснулись также субъектов критической информационной инфраструктуры, статус которых определен в Федеральном законе от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – Федеральный закон №187-ФЗ).

Национальное благополучие во многом сейчас зависит от безопасной и устойчивой критической инфраструктуры (системы и сети, лежащие в основе организации общества). Причинение критической информационной инфраструктуре (далее – КИИ) ущерба может привести к разрушающим и необратимым последствиям для их защищенности, а исходя из того, что КИИ выступает связующим звеном между другими областями национальной инфраструктуры, это неизбежно приведет к негативным для них последствиям.

В соответствии с Указом №166 Правительство РФ определило сроки и порядок перехода субъектов КИИ на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах КИИ, в соответствии с которыми такой переход на отечественное ПО должен быть осуществлен до 1 января 2030. Непосредственные мероприятия будут осуществляться с 01.09.2024.

В соответствии с ФЗ «О рынке ценных бумаг» профессиональными участниками рынка ценных бумаг являются юридические лица, которые созданы в соответствии с законодательством Российской Федерации и осуществляют следующие виды деятельности:

1. Брокерская деятельность;
2. Дилерская деятельность;
3. Деятельность форекс-дилера
4. Деятельность по управлению ценными бумагами
5. Депозитарная деятельность
6. Деятельность по ведению реестра владельцев ценных бумаг

Банк России контролирует деятельность профессиональных участников рынка ценных бумаг. Деятельность профессиональных участников рынка ценных бумаг лицензируется.

Также профессиональные участники относятся к некредитным финансовым организация в соответствии со ст.76.1 Федерального закона от 10.07.2002 №86-ФЗ «О Центральном банке Российской Федерации (Банке России)».

Следует отметить, что профессиональные участники рынка ценных бумаг относятся к субъектам КИИ и на них распространяют своё действие вышеперечисленные указы Президента РФ. В соответствии с Федеральным законом №187-ФЗ к субъектам КИИ относятся государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином

законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, государственной регистрации прав на недвижимое имущество и сделок с ним, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

В дополнение к вышеуказанному регулированию Президентом РФ был принят указ 01.05.2022 №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», согласно которому организации, являющиеся субъектами критической информационной инфраструктуры, должны осуществить следующие организационные мероприятия:

- возложить на заместителя генерального директора организации полномочия по обеспечению информационной безопасности организации, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак, и реагированию на компьютерные инциденты;
- создать в организации структурное подразделение, осуществляющее функции по обеспечению информационной безопасности организации, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, либо возложить данные функции на существующее структурное подразделение;

Также для организаций допускается привлечение организаций к осуществлению мероприятий по обеспечению информационной безопасности. При этом привлекаемый организации должны иметь лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Как мы видим начатая государством Цифровая трансформация в первую очередь коснулось государственные структуры, стратегические отрасли и все отрасли экономики, связанные с КИИ. Данная трансформация ставит перед профессиональными участниками не только задачи технического и программного переоснащения, связанные также с внесением изменений в особенности управления в компании, но также связана с вопросами управления рисками информационной безопасности.

Управление рисками информационной безопасности в рамках нормативного регулирования системы внутреннего контроля и системы управления рисками в профессиональных участниках осуществляется в рамках управления операционным риском.

Под операционным риском понимается риск возникновения последствий, влекущих в том числе приостановление или прекращение оказания услуг, а также возникновения расходов (убытков) профессионального участника, обусловленных сбоями в работе программно-технических средств, несоответствием их функциональных возможностей виду деятельности, характеру и масштабу совершаемых операций профессионального участника, нарушениями процедур проведения внутренних операций или неэффективностью указанных процедур, некорректными действиями или бездействием работников профессионального участника и (или) воздействием внешних событий.

Для профессиональных участников особое значение имеет поддержание операционной надежности, позволяющей непрерывно, безопасно и своевременно оказывать услуги в рамках лицензируемой деятельности. Следует отметить, что Банк России в рамках регулирования деятельности некредитных финансовых организаций в своих нормативных актах также устанавливает требования к защите информации [10] и операционной надежности [11].

В соответствии с методическими рекомендациями СРО «ПАРТАД» «Об организации системы управления операционным риском в организациях учетной инфраструктуры» под событием операционного риска понимается событие фактической реализации операционного риска. Следует отметить, что события операционного риска подразделяются на значимые события операционного риска и существенные события операционного риска.

Значимые события операционного риска признаются события, признаваемые организацией значимыми, и (или) реализация которых привела к последствиям, указанным в п.1.2 Указания ЦБ РФ №4501-У, а также иные события операционного риска, соответствующие критериям, установленным организацией.

Критериями существенности последствий, установленными Банком России, к которым может привести реализация соответствующих видов рисков Профессионального участника, в целях признания их значимыми, являются:

· снижение собственных средств Профессионального участника ниже размера собственных средств, установленного Банком России;

· наступление оснований для применения мер по предупреждению банкротства Профессионального участника;

· наступление оснований для аннулирования лицензии Профессионального участника, за исключением аннулирования лицензии на основании заявления Профессионального участника;

· невозможность непрерывного осуществления дальнейшей деятельности.

Существенными событиями операционного риска признаются события, не относящиеся к значимым событиям операционного риска, но оказывающие негативное влияние на процессы организации, осуществляемые в рамках лицензируемой деятельности, а также иные события операционного риска, соответствующие критериям, установленным организацией.

В соответствии с Указанием №4501-У, а также рекомендациями Саморегулируемых организаций, например, «Типовым регламентом управления рисками НФО», принятым СРО «ПАРТАД» Профессиональный участник может дополнительно установить критерий существенности последствий, к которым может привести реализация соответствующих видов рисков Профессионального участника. Самым распространённым дополнительным критерием является убыток (в процентном отношении), равный или превышающий определённый % от размера собственных средств Профессионального участника.

В составе событий операционного риска выделяются события операционного риска, связанные с нарушением операционной надежности – события операционного риска или серии связанных событий операционного риска, вызванных информационными угрозами, которые привели к неоказанию или ненадлежащему оказанию Профессиональным участником услуг.

Можно выделить следующие подвиды рисков информационной безопасности в рамках операционного риска.

Риски нарушения операционной надежности, к которым относятся:

- несанкционированный доступ к защищаемой информации с целью осуществления операций лицами, не обладающими правом их осуществления; [1].
- несанкционированное использование субъектами доступа (работниками профессионального участника и работниками поставщиков услуг) предоставленных им полномочий, в том числе в отношении объектов информационной инфраструктуры;
- технологическая зависимость функционирования объектов информационной инфраструктуры общества от поставщиков услуг;
- зависимость обеспечения операционной надежности от субъектов доступа – работников общества, обладающих знаниями, опытом и компетенцией, которые отсутствуют у всех иных работников общества.

Технологические риски, к которым относятся:

утечка/потеря конфиденциальной информации, информации, составляющей коммерческую тайну, или персональные данные;

- необеспечение непрерывности деятельности;
- сбои в работе программного обеспечения;
- сбои в работе оборудования (ПК, серверное оборудование, средства связи);
- невозможность оперативного устранения последствий неисправностей оборудования;
- неисполнение оборудованием возложенных на него функций из-за отказов и нарушений в работе;
- самопроизвольные сбои в работе оборудования;
- отключение электроэнергии/ перепады напряжения;
- сбой технологического процесса и пр.

На основании проанализированных нормативно-правовых актов и общего обзора системы управления рисками в профессиональных участниках можно сделать вывод, что Российская Федерация встала с 2018 года на путь развития собственной отрасли информационных технологий и созданию базовых институтов, обеспечивающих функционирование в государстве независимой и надежной критической информационной инфраструктуры. В условиях агрессивной международной конкуренции на рынке технологий и обеспечения технологической безопасности, построение критической информационной инфраструктуры страны на отечественной технологической базе является залогом успешного достижения сформулированных Президентом РФ национальных целей. При этом внутреннему контролеру и должностному лицу по управлению рисками в рамках управления операционным и регуляторным риском, в ближайшие годы, необходимо будет осуществить значительную работу по организации контроля выполнения требований вышеуказанных Указов Президента РФ и принимаемых в соответствии с ними законов и подзаконных актов, а также организовать эффективный процесс организации мониторинга и управление рисками информационной безопасности в организации.

Список литературы:

1. Федеральный закон от 22.04.1996 №39-ФЗ (ред. от 11.03.2024) «О рынке ценных бумаг» – [Электронный ресурс]. – Режим доступа: СПС Консультант Плюс.
2. Федеральный закон от 10.07.2002 №86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (ред. от 23.04.2024) – [Электронный ресурс]. – Режим доступа: СПС Консультант Плюс.
3. Федеральный закон от 26.07.2017 №187-ФЗ (ред. от 10.07.2023) «О безопасности критической информационной инфраструктуры Российской Федерации» – [Электронный ресурс]. – Режим доступа: СПС Консультант Плюс.
4. Указ Президента РФ от 07.05.2024 №309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» – [Электронный ресурс]. – Режим доступа: СПС Консультант Плюс.
5. Указ Президента РФ от 07.05.2018 №204 (ред. от 21.07.2020) «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» – [Электронный ресурс]. – Режим доступа: СПС Консультант Плюс.
6. Указ Президента РФ от 30.03.2022 №166 (ред. от 22.11.2023) «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» – [Электронный ресурс]. – Режим доступа: СПС Консультант Плюс.

7. Указ Президента РФ 01.05.2022 №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» – [Электронный ресурс]. – Режим доступа: СПС Консультант Плюс.

8. Указание Банка России от 21.08.2017 №4501-У (ред. от 27.08.2019) «О требованиях к организации профессиональным участником рынка ценных бумаг системы управления рисками, связанными с осуществлением профессиональной деятельности на рынке ценных бумаг и с осуществлением операций с собственным имуществом, в зависимости от вида деятельности и характера совершаемых операций» – [Электронный ресурс]. – Режим доступа: СПС Консультант Плюс.

9. Методические рекомендациями СРО «ПАРТАД» «Об организации системы управления операционным риском в организациях учетной инфраструктуры» – [Электронный ресурс]. – Режим доступа: https://partad.ru/UploadFiles/GetUploadedPdfFile?uploadFileId=1522

10. Положение Банка России от 20.04.2021 № 757-П (ред. от 20.04.2021) «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» – [Электронный ресурс]. – Режим доступа: СПС Консультант Плюс.

11. Положение Банка России от 15.11.2021 № 779-П «Об установлении обязательных для некредитных финансовых организаций требований к операционной надежности при осуществлении видов деятельности, предусмотренных частью первой статьи 761 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)» – [Электронный ресурс]. – Режим доступа: СПС Консультант Плюс.