УТВЕРЖДЕН

Приказом ПАО Московская Биржа

от «11» 07 2020 г. № МБ-П-2020-1767

Порядок защиты и раскрытия информации оператором финансовой платформы Публичным акционерным обществом «Московская Биржа ММВБ-РТС»

Оглавление

1. Общие положения

Порядок защиты и раскрытия информации (далее – Порядок) определяет способы хранения, защиты и правила раскрытия информации при осуществлении ПАО Московская Биржа (далее – Биржа) деятельности в качестве оператора финансовой платформы.

В целях настоящего Порядка применяются следующие термины и определения:

- *Информационная система* – совокупность взаимосвязанных программно-аппаратных средств, составляющая подсистему программно-технического комплекса Биржи и реализующая информационную технологию выполнения функций оператора финансовой платформы
- *Вредоносное программное обеспечение (вредоносное ПО)* – программное обеспечение, способное нарушить информационную безопасность информационной инфраструктуры Биржи.
- *Финансовая платформа* – информационная система, использующая программно-технические средства, предназначенные для обеспечения взаимодействия Участников и Финансовых организаций посредством информационно-телекоммуникационной сети «Интернет» в целях обеспечения возможности совершения финансовых сделок.
- *Пользователь (Пользователи)* – работники Биржи, а также клиенты, имеющие право доступа к финансовой платформе в соответствии с их полномочиями, установленными требованиями настоящего Порядка, иных внутренних документов Биржи, а также договорами, заключенными Биржей в связи с осуществлением своей деятельности в качестве оператора финансовой платформы;
- *Бизнес-владелец информационного ресурса* – руководитель подразделения, который в соответствии со своими должностными обязанностями отвечает за информацию, содержащуюся в конкретном информационном ресурсе или системе.

К информации, которая подлежит защите в соответствии с настоящим Порядком (далее – информация), относятся сведения, которые составляют конфиденциальную информацию, в том числе сведения, содержащиеся в финансовой платформе, а также иные не являющиеся общедоступными сведения, связанные с осуществлением деятельности Биржи в качестве оператора финансовой платформы.

Биржа осуществляет хранение и защиту информации, связанной со своей деятельностью в качестве оператора финансовой платформы, в том числе путем создания резервной копии (дублированного хранения информации) и наличия процедур, направленных на предотвращение технических сбоев и ошибок в части хранения и защиты информации, содержащейся в финансовой платформе.

Ответственность за разработку и осуществление мер, направленных на предотвращение неправомерного использования защищаемой информации, возлагается на Департамент операционных рисков, информационной

безопасности и непрерывности бизнеса в части электронной обработки и электронного хранения защищаемой информации;

Термины и определения, специально не определенные в настоящем Порядке, используются в значениях, установленных внутренними документами Биржи, а также законами, нормативными правовыми актами уполномоченного федерального органа исполнительной власти и иными нормативными правовыми актами Российской Федерации.

2. Обеспечение защиты информации при управлении доступом и регистрацией

Предоставление доступа к информационным ресурсам осуществляется в соответствии с требованиями, изложенными в документах «Политика управления доступом к информационным системам» и «Процедура изменения прав доступа к информационным системам» и основано на следующих принципах:

- Предоставление (изменение) доступа возможно только на основе заявки с обоснованием необходимости запрашиваемого доступа и одобренной руководителем соответствующего подразделения. При этом данная заявка в обязательном порядке согласовывается с Бизнес-владельцем информационного ресурса, к которому запрашивается доступ, а также с Департаментом операционных рисков информационной безопасности и непрерывности бизнеса. При необходимости, заявка согласовывается с лицом, находящемся в непосредственном подчинении у Председателя Правления и курирующем деятельность подразделения, в котором числится работник, запрашивающий доступ.
- Права доступа могут быть изменены в следующих случаях:
  - для выполнения работником должностных или договорных обязанностей;
  - в случае увольнения работника Биржи или прекращения деятельности представителя внешней стороны;
  - в случае перевода работника в другое подразделение внутри Биржи;
  - при выполнении процедуры мониторинга учетных записей и прав доступа к информационным системам;
  - при расследовании или предупреждении инцидента ИБ.
- Непосредственный доступ к информации, представленной на бумажных носителях, осуществляется руководителями подразделений, отвечающих за обеспечение работы с указанной информацией, на которых возложены обязанности по организации непосредственного доступа к указанным сведениям.

3. Обеспечение защиты информации на этапах жизненного цикла финансовой платформы

Процесс обеспечения информационной безопасности и защиты информации осуществляется в соответствии с требованиями «Политики внесения изменений в информационную структуру» и «Процедурой обеспечения информационной безопасности при внедрении новых проектов в информационной инфраструктуре» и охватывает следующие стадии жизненного цикла:

- Разработка технического задания;

  На стадии разработки технического задания должны быть определены функциональные требования и требования по информационной безопасности. Техническое задание должно быть согласовано с Департаментом операционных рисков информационной безопасности и непрерывности бизнеса в части информационной безопасности

- Проектирование;

  Подразделением, ответственным за проектирование, совместно с Департаментом операционных рисков информационной безопасности и непрерывности бизнеса, определяются:

  - структура и характеристики разрабатываемой системы, состав технических и программных средств, в том числе средств защиты информации,
  - требования к настройке и эксплуатации этих средств, параметры их взаимодействия,

  Кроме того, осуществляется проверка разрабатываемого программного кода на наличие уязвимостей.

- Разработка и тестирование;

  На данном этапе применяются следующие меры, направленные на обеспечение безопасности данного процесса:

  - разработка осуществляется в специально выделенных сегментах корпоративной сети Биржи и на рабочих местах ограниченного доступа;
  - для разработки применяются только лицензионные средства разработки и отладки программного кода;
  - разработка осуществляется на основании планов и методов, определенных на стадиях разработки технического задания и проектирования.
  - при проведении тестирования осуществляются проверка логики работы программного кода, в том числе входных и выходных данных, целостности информации, а также контроль внутренней обработки данных.
  - в тестовой среде не должны использоваться данные, которые могут содержать конфиденциальную информацию в противном случае должны применяться следующие защитные меры:

- перенос таких данных в тестовую среду осуществляется только при согласовании с руководителем подразделения ответственного за разработку и тестирование подразделения;
- доступ к тестовым средам ограничен и предоставляется в соответствии с «Политикой управления доступом к информационным системам» и «Процедурой изменения прав доступа к информационным системам»
- осуществляется регистрация действий с тестовой средой на уровне операционных систем;
- после завершения тестирования обеспечивается незамедлительное удаление данных.

- разработчикам запрещается проводить приемочное тестирование собственных разработок, а проводящий тестирование персонал не имеет прав на ввод новых версий систем в эксплуатацию без согласования.

- Приемка и ввод в эксплуатацию;

  Приемочные испытания включают следующие виды проверок:

  - правильности функционирования финансовой платформы при выполнении каждой функции;
  - качества реализации защитных мер;
  - совместимости финансовой платформы с уже эксплуатируемыми техническими средтсвами и отсутствия конфликтов между ними;
  - полноты и качества документации.

  На стадии ввода в эксплуатацию финансовой платформы должны быть выполнены настройки средств и механизмов обеспечения безопасности.

- Сопровождение и модернизация;

  Любые действия, связанные с внесением изменений в параметры функционирования финансовой платформы, в том числе в параметры реализованных мер, осуществляются только уполномоченными специалистами, и в порядке, установленном в «Политике внесения изменений в информационную структуру». Данный порядок предусматривает обязательное согласование вносимых изменений с Комитетом по согласованию технологических изменений.

4. Обеспечение защиты информации средствами антивирусной защиты

Обеспечение защиты информации средствами антивирусной защиты осуществляется в соответствии с требованиями «Политики защиты от вредоносного программного обеспечения» и «Процедурой защиты от вредоносного программного обеспечения» и состоит в следующем:

- внедрение и корректное функционирование системы антивирусной защиты с регулярным обновлением вирусных баз.
- запрет пользователям:
  - работать в информационной инфраструктуре (в том числе удаленно) без корректно функционирующих средств антивирусной защиты, а также с устаревшими обновлениями антивирусных баз;
  - самостоятельно отключать или удалять средства антивирусной защиты
- обязательный контроль на отсутствие вредоносного ПО любой информации (текстовые файлы любых форматов, файлы данных, исполняемые файлы, файлы архивов и т.п.) хранимой на рабочих станциях и серверах, получаемых и передаваемых по телекоммуникационным каналам, а также информации на съемных носителях (USB-накопителях, магнитных дисках, лентах, компакт-дисках и т.п.)
- проверку установочных файлов любого устанавливаемого на рабочие станции или серверы программного обеспечения на предмет отсутствия вредоносного ПО.
- проверка на отсутствие вредоносного ПО почтовых сообщений, WEB-трафика, а также файлов, в режиме реального времени и по расписанию, включая, сканирование всех файлов на жестком диске на предмет заражения.
- централизованное управление и регулярное обновление всех средств антивирусной защиты с применением механизма автоматического обновления.

5. Обеспечение защиты информации при использовании ресурсов информационно-телекоммуникационной сети «Интернет»

Обеспечение защиты информации при использовании ресурсов сети Интернет осуществляется в соответствии с требованиями документов «Политика пользования сетью Интернет» и «Политика допустимого использования информационных активов». Меры защиты включают в себя следующее:

- разрешение работникам Биржи использование ресурсов сети Интернет только в производственных целях
- для доступа к сети Интернет используется только разрешенное программное обеспечение, доступ к сети Интернет с использованием стороннего программного обеспечения запрещен.
- запрет использования внешних почтовых систем (например, mail.ru, gmail, hotmail) для выполнения должностных обязанностей
- запрет использование сторонних сервисов «мгновенных» сообщений (например, ICQ, MSN Messenger, Mail.ru агент, Google Chat), а также сторонних сервисов голосовых сообщений и интернет-телефонии
- технические меры, предотвращающие доступ работников к ресурсам и сервисам сети Интернет, относящихся на Бирже к запрещённым

6. Обеспечение защиты информации с использованием средств криптографической защиты информации

Средства криптографической защиты информации (далее СКЗИ) должны использоваться для обеспечения конфиденциальности и целостности информации, а также для обеспечения юридической значимости информации при совершении сделок или иных юридически значимых действий.

В соответствии с «Политикой криптографической защиты информации» СКЗИ могут использоваться для защиты:

- информации, хранимой на мобильных устройствах;
- информации, хранимой на рабочих станциях;
- информации, хранимой на съемных носителях;
- информации, обрабатываемой в информационных системах;
- информации, передаваемой по открытым каналам связи;
- информации, передаваемой при удаленном доступе к информационным ресурсам.

Тип СКЗИ, применяемых для шифрования информации, должен согласовываться с Департаментом операционных рисков информационной безопасности и непрерывности бизнеса. В случае использования алгоритмов шифрования, основанных на использовании пароля, такой пароль необходимо выбирать согласно «Политике парольной защиты»

Для защиты криптографических ключей должна обеспечиваться информационная безопасность процессов их изготовления, которая включает в себя комплекс технологических, организационных, технических и программных мер и средств защиты.

Персоналом, ответственным за изготовление, учет и использование криптографических ключей, должно обеспечиваться их безопасное хранение. Доступ неуполномоченных лиц к носителям криптографических ключей должен быть исключен.

Для обеспечения защиты электронных документов при совершении юридически значимых действий используется Система электронного документооборота. Организации и порядок информационного взаимодействия в процессе электронного документооборота, регламентируются «Правилами электронного документооборота» опубликованными на сайте Бирже в сети Интернет (http://www.moex.com).

7. Обеспечение защиты информации при назначении и распределении ролей

Защита информации при назначении и распределении ролей достигается посредством следующих мер:

- реализацией принципа "Знай своего клиента/контрагента"
- разграничением прав и обязанностей работников Биржи в соответствии с принципом «запрещено всё, что не разрешено явно»;
- наличием должностной инструкции для каждого работника Биржи, определяющей его функциональные обязанности;
- принципом обоснованности доступа, т.е. предоставлением доступа только к сведениям, необходимым работникам Биржи для выполнения своих должностных обязанностей в пределах предоставленных полномочий;
- индивидуальной идентификация пользователей, т.е. установление за ними идентификатора (учетной записи), на основе которого будет осуществляться разграничение доступа в соответствии с принципом обоснованности доступа;
- наличием подписанного работником Биржи соглашения о конфиденциальности, содержащего запрет на неправомерное использование сведений, составляющих служебную информацию и коммерческую тайну, и их разглашение;
- наличие утвержденных внутренних документов, устанавливающих режим работы со сведениями, составляющими коммерческую тайну.
- установлением перечня лиц, имеющих доступ к сведениям, относящимся к деятельности финансовой платформы

Все действия по изменению прав доступа работников Биржи к информационным ресурсам должны выполняться в порядке, регламентированном «Процедурой изменения прав доступа к информационным системам»

8. Организация деятельности службы информационной безопасности

Приоритеты, принципы и методы обеспечения информационной безопасности, в условиях наличия угроз, характерных и существенных для систем и информационных технологий Биржи содержатся в «Политике управления информационной безопасностью Публичного акционерного общества «Московская Биржа ММВБ-РТС».

Основной целью деятельности по обеспечению ИБ является достижение адекватной защищенности бизнес процессов Биржи и минимизация рисков ИБ. Для этого на Бирже обеспечивается решение следующих задач:

- инвентаризация и классификация информационных активов;
- внедрение процессов определения, оценки и обработки рисков;
- формирование и совершенствование системы управления информационной безопасности, в том числе процессов оценки и анализа ИБ;
- определение и документирование основных требований и процедур обеспечения ИБ;
- внедрение и настройка средств защиты информации;
- обучение персонала в области ИБ;
- своевременное выявление и устранение уязвимостей в информационных системах и тем самым предупреждение возможности нанесения ущерба и нарушения нормального функционирования бизнес-процессов в результате реализации угроз ИБ;
- уменьшение до приемлемого уровня возможного ущерба при реализации угроз ИБ, в том числе сокращение времени восстановления бизнес-процессов после возможных прерываний;
- планирование и оптимизация затрат на обеспечение ИБ.

Для реализации, эксплуатации, контроля и поддержания на должном уровне ИБ на Бирже сформирован Департамент операционных рисков информационной безопасности и непрерывности бизнеса, осуществляющий свою деятельность по следующим направлениям:

- информационная безопасность,
- обеспечение непрерывности бизнеса;
- операционные риски

С целью координации структурных подразделений Биржи при реализации мер информационной безопасности действует Комитет по информационной безопасности и непрерывности бизнеса.

9. Управление рисками нарушения защиты информации

В целях создания эффективной системы управления ИБ и достижения адекватной защищенности финансовой платформы, на Бирже реализуется деятельность по управлению рисками ИБ, которая является неотъемлемой частью всей деятельности по обеспечению ИБ и представляет собой непрерывный и цикличный процесс, включающий в себя совокупность следующих операций:

- определение контекста управления рисками
- оценка рисков.
- коммуникация рисков.
- обработка рисков
- мониторинг и пересмотр рисков

В соответствии с «Методикой оценки рисков информационной безопасности» оценка рисков включает в себя следующие последовательные стадии:

- идентификация угроз ИБ в отношении оцениваемого информационного актива и их источников;
- идентификация уязвимостей, присущих оцениваемому информационному активу, благодаря которым становится возможной реализация угроз ИБ в отношении данного актива;
- оценка степени тяжести последствий от реализации угрозы ИБ в отношении оцениваемого информационного актива;
- оценка вероятности реализации угрозы ИБ в отношении оцениваемого информационного актива
- расчет уровня риска

По итогам оценивания рисков ИБ составляется перечень недопустимых рисков, подлежащий дальнейшей обработке в соответствии с требованиями «Процедуры управления рисками информационной безопасности».

10. Регламентация и документирование деятельности по обеспечению защиты информации

Документирование деятельности по обеспечению защиты информации осуществляется в соответствии с установленными на Бирже требованиями к документообороту, изложенными в «Инструкции по делопроизводству» и дополненными в «Политике управления документацией системы управления информационной безопасностью», которые включают в себя:

- требования к подготовке, учету, хранению и оформлению документов
- требования к обеспечению сохранности документации и порядку доступа к ней
- требования к согласованности между собой всех положений документации по обеспечению ИБ и отсутствию противоречий с положениями «Политики управления информационной безопасностью Публичного акционерного общества «Московская Биржа ММВБ-РТС»
- требования к порядку пересмотра действующих документов и внесения в них изменений

В процессе функционирования системы управления информационной безопасностью должны создаваться записи с целью определения соответствия принятым требованиям по обеспечению информационной безопасности, а также анализа ее эффективности для последующего совершенствования. Записями являются любые документы или иные зафиксированные свидетельства о выполнении требований внутренних документов и/или об исполнении действий в процессах управления ИБ. Записями могут служить, в том числе, журналы аудита событий информационных систем, иные записи, представленные в электронном и/ или бумажном виде.

Записи должны сохраняться, защищаться и быть доступными в течение всего срока их хранения в соответствии с требованиями законодательства и других нормативных документов Биржи. Защита электронных записей осуществляется при помощи средств разграничения доступа и в соответствии с требованиями, изложенными в документах «Политика управления доступом к информационным системам» и «Процедура изменения прав доступа к информационным системам». Записи на бумажных и/или на отчуждаемых магнитных носителях , содержащие сведения, составляющие служебную информацию и/или коммерческую тайну хранятся в запираемых сейфах, шкафах (как правило, металлических), файл-боксах или в специально оборудованных помещениях;

11. Повышение осведомленности работников в области обеспечения защиты информации

Повышение осведомленности работников в сфере ИБ осуществляется в соответствии с требованиями «Политики повышения уровня осведомленности пользователей в области информационной безопасности» и включает в себя следующее:

- документы по обеспечению ИБ, непосредственно связанные с трудовой деятельностью работников, публикуются на внутреннем корпоративном ресурсе (портале) и доступны всем работникам Биржи для ознакомления.
- при приеме сотрудника на работу с ним проводится вводный инструктаж по соблюдению требований ИБ под подпись.
- работники Биржи проходят регулярное обучение (повышение уровня знаний) в области ИБ
- работники Биржи, ответственные за определение и контроль требований по ИБ должны постоянно поддерживать уровень своей компетенции.
- проводится периодический контроль знаний работников Биржи в области ИБ.
- правила информационной безопасности размещены на внутреннем портале и доступны всем работникам Биржи

12. Обнаружение инцидентов информационной безопасности и реагирование на них

Управление инцидентами ИБ связанными с деятельностью финансовой платформы осуществляется в соответствии с «Политикой управления инцидентами информационной безопасности», которая определяет требования к порядку регистрации инцидентов ИБ, сбора информации об инцидентах ИБ и выявлению предпосылок их возникновения для минимизации негативных последствий и предотвращения их повторного возникновения. Управление инцидентами ИБ включает в себя:

- критерии выявления инцидентов ИБ
- проведение сбора и анализа информации об инцидентах в ходе которого определяются вовлеченные информационные активы, круг предполагаемых нарушителей, условия и факторы возникновения инцидента ИБ
- классификацию (категоризацию) инцидентов с целью оперативного принятия оптимальных корректирующих действий, направленных на снижение ущерба и вероятности их повторного возникновения
- порядок регистрации инцидентов
- оценку степени серьезности инцидента (негативные последствия) в соответствии с принятой шкалой качественной оценки уровня негативных последствий
- проведение (в случае необходимости) служебных расследований в отношении нарушений ИБ, связанных с информационными активами
- устранение последствий инцидентов и принятие превентивных мер по недопущению инцидента в дальнейшем
- анализ статистики инцидентов для определения повторяющихся или особенно критичных инцидентов и принятия решений по выработке предупреждающих и корректирующих действий.

В общем виде концепцию по управлению инцидентами в отношении финансовой платформы можно представить, как единый постоянно функционирующий циклический процесс, состоящий из следующих элементов:

- Контроль доступов и сетевой защищенности
- Контроль соответствия Участников правилам и требованиям Платформы
- Контроль и актуализация бизнес процессов
- Мониторинг совершаемых транзакций (фрод-мониторинг)
- Сбор и анализ данных об инцидентах
- Обеспечение непрерывности деятельности Платформы

В данный процесс вовлечены все подразделения МБ, обеспечивающих эксплуатацию и сопровождение Платформы. Функциональные обязанности данных подразделений определяются их внутренними регламентами.

Ключевая роль в управлении рисками Платформы отводится Департаменту операционных рисков, информационной безопасности и непрерывности бизнеса, который помимо управления информационной безопасностью системы координирует действия подразделений группы компаний Московская биржа при устранении последствий выявленных инцидентов и нештатных ситуаций.

В целях мониторинга информационной безопасности финансовой платформы в структуре ДОРИБиНБ функционирует специализированное подразделение Security operation center (SOC), которое осуществляет мониторинг событий информационной безопасности в режиме реального времени. Мониторинг осуществляется с помощью штатных средств, входящих в технологический стек ПАО «Московская биржа».

Каждое событие информационной безопасности в системе (в независимости от того успешное оно или нет) должно быть зарегистрировано в системе. Минимальный набор атрибутов для регистрируемого события должен включать:

- дата/время события
- результат события (успех/отказ)
- идентификатор источника события (имя учетной записи, адрес, Id)
- идентификатор объекта доступа
- тип доступа к объекту

В случае выявления риска (регистрации инцидента) ответственные подразделения выполняют действия по устранению последствий инцидента в соответствии с возложенными на них функциональными обязанностями. При отсутствии типового решения определяется круг вовлечённых подразделений и осуществляется запрос дополнительной информации по инциденту у других подразделений, обеспечивающих сопровождение МП. В случае необходимости производится эскалация на руководителей ответственных подразделений, разработчика М, ответственных лиц представляющих организации Участников Платформы и Платежных систем.

В целях обеспечения защиты информации при совершении финансовых сделок с использованием финансовой платформы ПАО Московская Биржа, как оператор финансовой платформы, реализует мероприятия по выявлению финансовых сделок с использованием финансовой платформы без волеизъявления участников, а также организует формирование и ведение базы данных о таких сделках и попытках осуществления несанкционированных операций.

13. Мониторинг и анализ обеспечения защиты информации

На Бирже должен регулярно проводиться мониторинг и анализ эффективности информационной безопасности финансовой платформы. Целями такого мониторинга является:

- выявление ошибок в результатах обработки информации
- выявление удачных и неудавшихся попыток нарушений и инцидентов информационной безопасности
- выявление мошеннических действий

Мониторинг и анализ обеспечения защиты информации может проводиться, как с использованием специальных технических и программных средств контроля, так и без них.

В соответствии с «Процедурой анализа эффективности и совершенствования системы управления информационной безопасности» деятельность по анализу эффективности процессов управления информационной безопасностью возлагается на Комитет информационной безопасности и непрерывности бизнеса, который на основе полученных результатов проведения аудитов безопасности, статистики по инцидентам ИБ, проводит такой анализ в рамках своих заседаний.

14. Своевременное совершенствование обеспечения защиты информации.

Процесс обеспечения защиты информации должен постоянно совершенствоваться путем применения корректирующих и предупреждающих мер, определенных по результатам анализа системы управления информационной безопасностью. Порядок выбора, согласования и применения, корректирующих и предупреждающих мер должен быть документирован.

Меры по совершенствованию обеспечения информационной безопасности на Бирже сформулированы в «Политике управления информационной безопасностью Публичного акционерного общества «Московская Биржа ММВБ-РТС», их реализация на практике заключаются в следующем:

- распределение функций и ответственности работников Биржи в сфере обеспечения информационной безопасности;
- управление документацией системы управления информационной безопасностью;
- управление рисками информационной безопасности;
- мониторинг, анализ эффективности и совершенствование процессов системы управления информационной безопасности;
- обеспечение информационной безопасности при работе с персоналом;
- повышение уровня знаний и контроль знаний работников Биржи в области информационной безопасности;
- организация работы со сторонними организациями;
- обеспечение физической безопасности и защита оборудования;
- технические и организационные меры обеспечения информационной безопасности;
- управление инцидентами информационной безопасности;
- управление непрерывностью бизнеса;
- соблюдение требований законодательства;
- использование лицензионного программного обеспечения;
- внутренние аудиты информационной безопасности.

15. Меры, направленные на защиту финансовой платформы от ошибок и несанкционированного доступа

С целью обеспечения конфиденциальности, целостности и доступности финансовой платформы, а также предотвращения сбоев и ошибок, Биржей реализуются меры защиты, включающие в себя:

- организационные (административные) меры и условия эксплуатации программно-технических средств финансовой платформы
- технические меры защиты, программно-технических средств, финансовой платформы.

В состав организационных (административных) мер входит:

- при кабинетной планировке помещений:
  - ограничение доступа посторонних лиц в помещения Биржи, в которых расположены рабочие места работников структурных подразделений Биржи, непосредственно осуществляющих функции, связанные с управлением финансовой платформы, а также в иные помещения Биржи, предусматривающие возможность эксплуатации и получения информации из финансовой платформы, включая:
    - оборудование системой контроля и управления доступом помещений Биржи, в которых устанавливаются рабочие места, предназначенные для обработки конфиденциальной информации содержащейся в финансовой платформе
    - размещение рабочих мест для работников Биржи и установка оборудования финансовой платформы способом, исключающим возможность бесконтрольного наблюдения за работой или непосредственного проникновения в эти помещения и доступа к находящемуся в них оборудованию посторонних лиц;
    - установление пропускного и внутриобъектного режима, исключающего проникновение в здания и помещения Биржи посторонних лиц, а также, предусматривающего, в том числе, совокупность мероприятий, требований и правил, определяющих режим допуска в помещения Биржи, в которых установлены рабочие места, а также иное оборудование, входящее в состав финансовой платформы;
- при открытой планировке (open space):
  - установка рабочих мест для работников Биржи, которые имеют доступ конфиденциальной информации и доступ к финансовой платформе, при которой условия оснащения таких рабочих мест аппаратно-программными комплексами защиты от несанкционированного доступа и их размещение исключают возможность просмотра со стороны других работников Биржи и иных лиц.
  - установление порядка доступа к финансовой платформе, включая:
    - определение в должностных инструкциях работников Биржи

их прав и обязанностей при работе с финансовой платформой;

- предоставление доступа к финансовой платформе только ограниченному кругу работников Биржи в соответствии с предоставленными им правами, обеспечивающими осуществление доступа только к сведениям, необходимым им для выполнения своих должностных обязанностей в пределах предоставленных полномочий;
- организацию доступа работников Биржи к финансовой платформе только с определенного рабочего места (рабочих мест);
- контроль за ведением автоматизированного журнала регистрации пользователей в финансовой платформе и регистрации попыток несанкционированного доступа.

- проведение Департаментом операционных рисков информационной безопасности и непрерывности бизнеса, не реже одного раза в год выверки (контроля актуальности) списков лиц, допущенных к работе, с информацией, содержащейся в финансовой платформе.

В состав технических мер защиты программно-технического комплекса, финансовой платформы, входит:

- географическое разнесение основного и резервного вычислительных центров (далее – ВЦ), обеспечивающее катастрофоустойчивость и непрерывность функционирования финансовой платформы;
- физическая защита основного и резервного ВЦ, обеспечивающая защиту программно-технического комплекса от повреждений и несанкционированного доступа со стороны лиц, для которых этот доступ не разрешен, а также от воздействия внешних агрессивных факторов, которая предусматривает:
  - расположение вычислительных средств только в охраняемых помещениях с ограниченным доступом (далее – специальные помещения);
  - оборудование специальных помещений средствами защиты и системами безопасности (усиленными дверьми, защищенными оконными проемами и вентиляционными отверстиями, системами контроля доступа, пожарной и охранной сигнализацией, телевизионного наблюдения);
  - оборудование специальных помещений во избежание воздействия внешних агрессивных факторов автоматической системой пожаротушения и поддержания микроклимата;
  - оборудование специальных помещений в целях поддержания бесперебойного функционирования ВЦ сдвоенной системой бесперебойного электропитания;
- логическая сегментация сети с использованием межсетевых экранов, исключающая несанкционированный доступ к информации финансовой платформы через нестандартные порты, протоколы или

аппаратное обеспечение;

- использование кластерного решения на базе аппаратной платформы и среды виртуализации;
- проведение регулярных тестов на проникновение и анализа исходного кода;
- установление механизма защиты от несанкционированного доступа на уровне программного обеспечения, включающего:
  - строгую идентификация /аутентификацию;
  - использование электронных подписей на всех этапах процесса обработки информации в финансовой платформе и при выполнении действий, влияющих на статус, изменение информации финансовой/банковской операции;
  - контроль точности, полноты и правильности входных данных
  - протоколирование всех действий персонала/сервисов/Клиентов, участников обмена, в т.ч. фактов изменения статуса, информации финансовой/банковской операции;
  - цифровое согласие пользователя.
- защита от уничтожения и искажения информации, при возникновении сбоев и ошибок, а также в случаях некорректных действий пользователей финансовой платформы
- наличие технологии хранения и восстановления информации, включающую процедуру регулярного копирования и хранения архивных копий данных финансовой платформы, перед и/или после проведения основных технологических работ с ней

16. Правила раскрытия информации

Следующая информация, обрабатываемая Биржей, является конфиденциальной:

- информация, содержащаяся в документах, составляемых в электронном виде Биржей, как оператором финансовой платформы, потребителем финансовых услуг, регистратором финансовых транзакций при совершении финансовых сделок;
- информация обо всех совершенных финансовых сделках, а также о расчетах по финансовым сделкам, предоставленная Биржей, как оператором финансовой платформы регистратору финансовых транзакций.
- информация, содержащейся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками или клиентами Биржи;
- информация, необходимая Бирже для авторизации своих клиентов в целях осуществления финансовых операций и удостоверения права

клиентов распоряжаться денежными средствами, ценными бумагами или иным имуществом;

- информации об осуществленных Биржей и её их клиентами финансовых операциях;
- используемая при осуществлении финансовых операций ключевая информация средств криптографической защиты информации.

Указанная информация, не подлежит разглашению и несанкционированной передаче или иному публичному раскрытию в любых информационных источниках и может передаваться в следующих случаях :

- сотрудникам Биржи в объеме, необходимом для исполнения ими своих служебных обязанностей,
- органам государственной власти в случаях и объеме, предусмотренных действующим законодательством,

Согласно Процедуре учета, хранения и уничтожения конфиденциальной информации, персональные данные относятся к конфиденциальной информации.

Передача персональных данных, обрабатываемых финансовой платформой, может осуществляться в следующих случаях:

- передача третьим лицам, с которыми Биржей заключены договоры, предполагающие передачу и обработку персональных данных, в целях обеспечения бизнес-процессов финансовой платформы
- выполнение работниками Биржи должностных обязанностей, связанных с обработкой персональных данных
- передача персональных данных на архивное хранение
- передача персональных данных в рамках федерального законодательства

При передаче вышеуказанных персональных данных должны быть соблюдены следующие правила:

- несанкционированный доступ к персональным данным в процессе передачи должен быть исключен;
- передача персональных данных возможна только в том случае, если обеспечивается конфиденциальность передаваемой информации;
- если Биржа на основании договора поручает обработку персональных данных третьей стороне, существенным условием договора является обязанность обеспечения третьей стороной конфиденциальности и безопасности персональных данных при их передаче;
- не сообщать персональные данные субъекта персональных данных третьей стороне без его письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, предусмотренных Трудовым Кодексом Российской Федерации и иными федеральными законами;

- не сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные субъектов персональных данных, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.
- передавать персональные данные субъектов персональных данных их представителям в порядке, установленном Трудовым Кодексом Российской Федерации и иными федеральными законами, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями субъектов персональных данных их функций.

Биржа, как оператор финансовой платформы:

- направляет в Банк России информацию обо всех случаях и (или) о попытках осуществления операций, направленных на совершение финансовых сделок с использованием финансовой платформы без волеизъявления участников финансовой платформы, по форме и в порядке, которые установлены Банком России.
- раскрывает на своем сайте в информационно-телекоммуникационной сети «Интернет», следующую информацию и документы:
- фирменное наименование оператора финансовой платформы, сведения о государственной регистрации юридического лица, сведения о регистрации оператора финансовой платформы в реестре операторов финансовых платформ;
- место нахождения оператора финансовой платформы;
- устав оператора финансовой платформы;
- правила финансовой платформы, сведения об их регистрации в Банке России;
- размер вознаграждения оператора финансовой платформы или порядок его определения, порядок уплаты такого вознаграждения;
- реквизиты специального счета или счетов оператора финансовой платформы (при наличии);
- перечень лиц, осуществляющих учет прав на ценные бумаги, передача прав на которые потребителям финансовых услуг осуществляется в результате совершения финансовых сделок, заключенных с использованием финансовой платформы;
- перечень лиц, привлекаемых Биржей, как оператором финансовой платформы на основании соглашения для обеспечения размещения в соответствии с правилами финансовой платформы информации о финансовых сделках, совершаемых с использованием финансовой платформы;

- перечень банков, которым Биржей, как оператором финансовой платформы поручено проведение идентификации клиентов - потребителей финансовых услуг при их личном присутствии, представителей клиентов, выгодоприобретателей, бенефициарных владельцев в целях заключения с такими клиентами договора об оказании услуг оператора финансовой платформы;
- сведения о выявленных конфликтах интересов и принятых мерах по минимизации риска их негативных последствий;
- информация о технических сбоях в функционировании программно-аппаратных средств, необходимых для оказания услуг Биржи, как оператора финансовой платформы, в том числе вследствие обстоятельств непреодолимой силы, которые повлекли за собой прекращение или ограничение работоспособности таких средств, что привело к отсутствию возможности осуществления оператором финансовой платформы своей деятельности в отношении всех участников финансовой платформы, с указанием даты, времени и причин прекращения работоспособности таких средств, а также информация о сроках восстановления функционирования программно-аппаратных средств;
- фирменные наименования и места нахождения финансовых организаций и эмитентов, являющихся участниками финансовой платформы;
- информация о расторжении договора об оказании услуг оператора финансовой платформы между Биржей, как оператором финансовой платформы и финансовой организацией или эмитентом и о последствиях расторжения такого договора;
- иная информация в случае, если требование о ее раскрытии установлено Банком России.
- правила финансовой платформы (после их регистрации в Банке России).