

УТВЕРЖДЕНО
Приказом Генерального директора
ПАО «СПБ Биржа»
№ 451 от 17.04.2023

**ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВАЛИДАТОРОВ, ПРИВЛЕКАЕМЫХ
ОПЕРАТОРОМ ИНФОРМАЦИОННОЙ СИСТЕМЫ
ПАО «СПБ БИРЖА»**

Москва
2023

1. Валидатор в значении, предусмотренном правилами информационной системы ПАО «СПБ Биржа» (далее – **Валидатор**), обеспечивает защиту информации, бесперебойность и непрерывность функционирования информационной системы, в которой осуществляется выпуск цифровых финансовых активов, эксплуатируемой ПАО «СПБ Биржа» (далее – **информационная система**) в своей части.

2. Валидатор пересматривает пороговые уровни показателей бесперебойности с использованием результатов оценки рисков в информационной системе не реже одного раза в год.

3. Для проведения работ по защите информации Валидатором могут привлекаться на договорной основе организации, имеющие лицензию на проведение работ и услуг, предусмотренных Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

4. Для защиты информации от воздействия вредоносного кода Валидатором используются средства антивирусной защиты с функцией централизованного управления, мониторинга и автоматического реагирования в случаях выявления вредоносного кода.

5. Валидатор должен обеспечить надлежащий уровень реагирования на инциденты информационной безопасности в соответствии с собственными внутренними регламентами.

6. Комплекс информационной безопасности должен содержать следующие основные компоненты:

6.1. Журналирование событий: непрерывная запись всех доступных событий системы для анализа, поддерживает системы точного времени, которая необходима для точной фиксации информационных событий;

6.2. Шифрование передачи данных: персональные, идентификационные и аутентификационные данные передаются исключительно с использованием шифрования в соответствии с требованиями законодательства;

6.3. Ограничение доступа: все пользователи информационной системы (в том числе работники Валидатора) получают персонализированный доступ к информационной системе с использованием аутентификационных данных.

7. Взаимодействие с Валидатором должно выполняться с использованием защищенных каналов связи.

8. В рамках реализации процессов взаимодействия пользователей информационной системы Валидатор выполняет следующие меры, направленные на обеспечение информационной безопасности:

8.1. Выделение отдельного контакта службы (подразделения), ответственного за выявление и устранение инцидентов информационной безопасности;

8.2. Регулярная, не реже одного раза в год, оценка уровня безопасности программно-технического комплекса Валидатора.

9. В рамках реализации процессов взаимодействия пользователей информационной системы Валидатор выполняет следующие меры, направленные на обеспечение операционной надежности:

9.1. Резервирование средств взаимодействия, включая каналы связи, аппаратное и программное обеспечение;

9.2. Проведение регулярного тестирования средств, обеспечивающих резервирование, не реже одного раза в год.

10. Валидатор обеспечивает защиту от проникновения, а именно: предотвращение вмешательства в работу Системы из общедоступных сетей передачи данных, в том числе из сети Интернет. Валидатор проводит анализ и ограничение (при необходимости) входящего и исходящего потока данных на соответствие требованиям правил безопасности.