УТВЕРЖДЕНО:
Решением Единоличного
исполнительного органа
ООО «Спутник ЦФА»
№ 20241022-2 от «22» октября 2024 г.

ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОПЕРАТОРА ОБМЕНА ЦИФРОВЫХ ФИНАНСОВЫХ АКТИВОВ, ПРИВЛЕКАЕМОГО ОПЕРАТОРОМ ИНФОРМАЦИОННОЙ СИСТЕМЫ ООО «СПУТНИК ЦФА»

г. Москва
2024 год

1. Оператор обмена цифровых финансовых активов в значении, предусмотренном в Федеральном законе от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – Оператор обмена), обеспечивает защиту информации, бесперебойность и непрерывность функционирования информационной системы, в которой осуществляется выпуск цифровых финансовых активов, эксплуатируемой ООО «Спутник ЦФА» (далее – информационная система) в своей части.

2. Оператор обмена 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 Оператором обмена 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 Оператором обмена используются средства антивирусной защиты с функцией централизованного управления, мониторинга и автоматического реагирования в случаях выявления вредоносного кода.

5. Оператор обмена 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 Оператора обмена) получают персонализированный доступ а информационную систему с использованием аутентификационных данных.

7. Взаимодействие с Оператором обмена должно выполняться с использованием защищенных каналов связи.

8. В рамках реализации процессов взаимодействия пользователей информационной системы Оператор обмена 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 Оператора обмена.

9. В рамках реализации процессов взаимодействия пользователей информационной системы Оператор обмена 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. Оператор обмена обеспечивает защиту от проникновения, а именно: предотвращение вмешательства в работу Системы из общедоступных сетей передачи данных, в том числе из сети Интернет. Оператор обмена проводит анализ и ограничение (при необходимости) входящего и исходящего потока данных на соответствие требованиям правил безопасности.

11. Программно-технические требования

Все серверы, ПО и иные вычислительные ресурсы информационной системы Оператора обмена (ИС) должны поддерживать работу в среде виртуализации и контейнеризации.

11.1. Требования к аппаратному обеспечению Платформы Оператора обмена

№	Наименование	Кол-во	Центральный процессор (кол-во ядер/частота)	ОЗУ (ГБ)	Требуемые объемы данных (ГБ) SSD
1	Узел системы	1	2 ядра / 2 ГГц	2 Гб	20
2	Адаптер системы	1	2 ядер / 2 ГГц	2 Гб	20

11.2. Требования к системному программному обеспечению.

ПЭВМ архитектуры x86, x64;

Операционная система с ядром Linux версии 3.0 и выше, рекомендуемый дистрибутив: Ubuntu 20.04 или выше;

СКЗИ «КриптоПро CSP», версия 5.0 R2 (КС1);

Набор криптографических библиотек cprocsp-pki-cades версии не ниже 2.0.

Допускается развертывание компонентов ПО в следующих виртуальных средах (только в случае использования СКЗИ «КриптоПро CSP» версии 5.0 КС1, исполнение 1-Base):

- Microsoft Hyper-V Server 2008/2008R2/2012/2012R2/2016 (x64);
- Microsoft Hyper-V 8/8.1/10 (x64);
- Citrix XenServer 7 (x64);
- VMWare WorkStation 11/12/14/15 (x86, x64);
- VMWare WorkStation Player 12/14/15 (x86, x64);
- VMWare vSphere ESXi/Hypervisor 5.5/6.0/6.5/6.7 (x64);
- RHEV 4 (x64);
- Платформа виртуализации серверов «Хост» (HOSTVM).

11.3. Требования к каналу связи:

- Скорость соединения не менее 20 МБит/сек.