УТВЕРЖДЕНО
Решением единственного акционера
Акционерного общества
«Универсальные Финансовые Технологии»
№ 3 от «05» сентября 2023 г.

ПРАВИЛА ЗАЩИТЫ И РАСКРЫТИЯ ИНФОРМАЦИИ ОПЕРАТОРОМ ФИНАНСОВОЙ ПЛАТФОРМЫ Акционерным обществом «Универсальные Финансовые Технологии»

Вступает в силу	
Редакция №	1

2023 г.

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Правила защиты и раскрытия информации (далее - Правила) определяют способы хранения, защиты и правила раскрытия информации при осуществлении Акционерным обществом «Универсальные Финансовые Технологии» (далее - Общество) деятельности в качестве Оператора финансовой платформы.

1.2. Общество осуществляет защиту следующей информации, получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой в автоматизированных системах, используемых Обществом:
1.2.1. информации, содержащейся в документах, составляемых при осуществлении финансовых сделок (операций) в электронном виде работниками Общества и/или Финансовыми организациями, Потребителями Общества (далее - Электронные сообщения);
1.2.2. информации, необходимой Обществу для авторизации своих Потребителей в целях осуществления финансовых сделок (операций) и удостоверения права Потребителей распоряжаться денежными средствами, ценными бумагами или иным имуществом;
1.2.3. информации об осуществленных Обществом и Потребителями финансовых сделок (операциях);
1.2.4. ключевой информации средств криптографической защиты информации, используемой Обществом и Потребителями, Финансовой организацией при осуществлении финансовых сделок (операций);
1.2.5. информации, обрабатываемой Обществом при совершении финансовых сделок (операций) с использованием Финансовой платформы;
1.2.6. информации, содержащейся в Электронных сообщениях, составляемых участниками Финансовой платформы, Оператором и Регистратором финансовых транзакций при заключении и исполнении финансовых сделок (операций) с использованием Финансовой платформы, в том числе содержащейся в Электронных сообщениях - указаниях Потребителей финансовых услуг;
1.2.7. информации о размещенных с использованием Финансовой платформы банковских вкладах и об операциях с денежными средствами по ним, информации о совершении иных финансовых сделок и об операциях по ним, предоставленной Обществом Регистратору финансовых транзакций;
1.2.8. Электронных сообщений, которые содержат распоряжения Общества кредитной организации о совершении сделок (операций) по специальному счету на основании указания Потребителя финансовых услуг.

1.3. Защита информации с помощью средств криптографической защиты информации (далее - СКЗИ) осуществляется Обществом в соответствии с технической документацией на СКЗИ и законодательством Российской Федерации.

1.4. Если в технической документации на СКЗИ установлены требования к оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, Общество проводит оценку выполнения предъявляемых к нему

требований в соответствии с Приказом ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)». Техническое задание согласовывается с федеральным органом исполнительной власти в области обеспечения безопасности.

1.5. Если Общество применяет СКЗИ российского производства, СКЗИ должны иметь сертификаты соответствия федерального органа исполнительной власти в области обеспечения безопасности.

1.6. Безопасность процессов изготовления криптографических ключей СКЗИ должна обеспечиваться комплексом технологических мер защиты информации, организационных мер защиты информации и технических средств защиты информации в соответствии с технической документацией на СКЗИ.

1.7. Общество осуществляет защиту информации в отношении эксплуатируемых автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 08.08.2017 №822-ст «Об утверждении национального стандарта Российской Федерации» (ГОСТ Р 57580.1-2017), а также по результатам определения Обществом реализуемого в течение календарного года уровня защиты информации.

1.8. Общество обеспечивает уровень соответствия не ниже третьего в соответствии с национальным стандартом Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 28.03.2018 № 156-ст «Об утверждении национального стандарта Российской Федерации» (ГОСТ Р 57580.2-2018).

1.9. Общество обеспечивает проведение оценки соответствия уровня защиты информации не реже 1 (одного) раза в 3 (три) года. Оценка соответствия уровня защиты информации должна осуществляться с привлечением сторонних организаций, имеющих лицензию на проведение соответствующих работ и услуг (проверяющая организация), и в соответствии с требованиями ГОСТ Р 57580.2-2018. Отчёт, составленный проверяющей организацией по результатам оценки соответствия уровня защиты информации, хранится в Обществе не менее 5 (пяти) лет с даты его выдачи проверяющей организацией.

2. СПИСОК ОПРЕДЕЛЕНИЙ И СОКРАЩЕНИЙ

Банк России - Центральный банк Российской Федерации, включая его территориальные подразделения;

Оператор финансовой платформы (ОФП) - Акционерное общество «Универсальные Финансовые Технологии» - юридическое лицо, созданное в организационно-правовой форме акционерного общества в соответствии с законодательством Российской Федерации, оказывающее услуги, связанные с обеспечением возможности совершения Финансовых сделок между Финансовыми организациями и Потребителями с использованием финансовой платформы, включенное в реестр операторов финансовых платформ Банка России;

Потребитель финансовых услуг, Потребитель - физическое лицо, являющееся потребителем финансовых услуг и соответствующее требованиям, установленным в Правилах финансовой платформы, присоединившееся к договору об оказании услуг Оператора финансовой платформы в порядке, установленном Правилами финансовой платформы, в целях совершения Финансовых сделок. Авторизовавшийся Пользователь считается Потребителем;

Правила финансовой платформы (Правила платформы) - документ, утвержденный решением единственного акционера Акционерного общества «Универсальные Финансовые Технологии» и зарегистрированный в установленном порядке в соответствии с Федеральным законом от 20.07.2020 № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы»;

Регистратор финансовых транзакций (РФТ) – небанковская кредитная организация акционерное общество «Национальный расчетный депозитарий» (ОГРН: 1027739132563)

Сайт финансовой платформы - сайт в информационно-телекоммуникационной сети «Интернет», используемый Оператором платформы для обеспечения возможности совершения финансовых сделок и взаимодействия между Оператором платформы, Финансовыми организациями, Потребителями и Пользователями. Адрес сайта платформы: www.fin-id.ru

СКЗИ – средства криптографической защиты информации;

Специальный счет - номинальный счет Оператора платформы, предназначенный для совершения операций с денежными средствами, принадлежащими бенефициарам – потребителям финансовых услуг (Потребителям) и используемый при совершении Финансовых сделок между Потребителями и Финансовыми организациями;

Финансовые организации - кредитные организации, Банки, присоединившиеся к договору об оказании услуг Оператора финансовой платформы, условия которого установлены Правилами финансовой платформы, в целях совершения Финансовых сделок с Потребителями;

Финансовая платформа (Платформа) - информационная система, которая обеспечивает взаимодействие финансовых организаций или эмитентов с потребителями финансовых услуг посредством информационно-телекоммуникационной сети «Интернет» в целях обеспечения возможности совершения финансовых сделок и доступ к которой предоставляется оператором финансовой платформы.

Финансовая сделка - сделка, совершаемая между Потребителями и Финансовыми организациями с использованием Финансовой платформы. Перечень финансовых сделок, заключение (совершение) которых возможно с использованием Финансовой платформы, устанавливается Правилами финансовой платформы.

3. ОТВЕТСТВЕННЫЕ ЛИЦА

Наименование	Ответственность
Все сотрудники Акционерного общества «Универсальные Финансовые Технологии»	персональная ответственность за соблюдение настоящих Правил
Генеральный директор	контроль за соблюдением настоящих Правил

Мониторинг своевременности актуализации настоящих Правил осуществляется комплексным контролером в рамках процедур по актуализации внутренних документов.

4. ОПРЕДЕЛЕНИЕ УРОВНЯ ЗАЩИТЫ ИНФОРМАЦИИ

4.1. Общество ежегодно не позднее 10 (десятого) рабочего дня каждого календарного года определяет уровень защиты информации.

4.2. Общество определяет уровень защиты информации в зависимости от количества лиц, которым Общество оказывало услуги в соответствии с заключёнными с такими лицами договорами об оказании услуг Оператора финансовой платформы в течение 3 (трех) последних кварталов по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации:

4.2.1. минимальный уровень защиты информации - не более 100 000 лиц;

4.2.2. стандартный уровень защиты информации - более 100 000 лиц.

4.3. Вне зависимости от реализуемого уровня защиты информации Общество обязано:

4.3.1. в целях противодействия незаконным финансовым операциям доводить до Потребителей финансовых услуг рекомендации по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средств вычислительной техники (далее - Вредоносный код);

4.3.2. доводить до Потребителей финансовых услуг информацию о возможных рисках несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления, а также информацию о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) Потребителем устройства, с использованием которого им совершались действия в целях осуществления финансовой сделки (операции), контролю конфигурации устройства и(или) действия в целях осуществления финансовой сделки (операции), и своевременному обнаружению воздействия Вредоносного кода;

4.3.3. осуществлять регистрацию инцидентов, связанных с обеспечением защиты информации при осуществлении деятельности в сфере финансовых рынков (далее по тексту

- Инциденты защиты информации), а также представлять сведения о выявленных Инцидентах защиты информации должностному лицу (отдельному структурному подразделению), ответственному за управление рисками;

4.3.4. обеспечивать подписание Электронных сообщений, в том числе договоров между Обществом как Оператором финансовой платформы и Потребителем финансовых услуг, соглашений об электронном документообороте между Обществом как Оператором финансовой платформы, Потребителем финансовых услуг и Финансовой организацией, а также иных документов, необходимых для обеспечения их взаимодействия при заключении и исполнении Финансовых сделок с использованием Финансовой платформы, способом, позволяющим обеспечить целостность подписываемых документов и подтвердить их составление уполномоченным на это лицом.

5. ТРЕБОВАНИЯ К ТЕХНОЛОГИИ ОБРАБОТКИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

5.1. Технология обработки защищаемой информации, применяемая Обществом при идентификации, аутентификации и авторизации Потребителей финансовых услуг в целях осуществления финансовых сделок, при формировании (подготовке), передаче и приёме Электронных сообщений, при удостоверении права Потребителей финансовых услуг распоряжаться денежными средствами, при осуществлении финансовой сделки, учете результатов её осуществления (при наличии учёта), при хранении Электронных сообщений и информации об осуществлённых финансовых сделках (далее при совместном упоминании – Технологические участки), должна обеспечивать целостность и неизменность защищаемой информации, в том числе путём:

5.1.1. применения при формировании и обмене Электронными сообщениями механизмов и(или) протоколов, обеспечивающих защиту Электронных сообщений от искажения, фальсификации, переадресации, несанкционированного ознакомления и(или) уничтожения, ложной авторизации, в том числе аутентификации входных Электронных сообщений;

5.1.2. взаимной (двухсторонней) аутентификации участников обмена Электронными сообщениями средствами вычислительной техники Общества, Потребителей финансовых услуг и Финансовых организаций;

5.1.3. восстановления защищаемой информации в случае умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;

5.1.4. применения СКЗИ, имеющих сертификаты соответствия федерального органа исполнительной власти в области обеспечения безопасности, при взаимодействии между Обществом и Регистратором финансовых транзакций, а также между Обществом и Финансовыми организациями.

5.2. Технология обработки защищаемой информации, применяемая Обществом при идентификации, аутентификации и авторизации, должна обеспечивать выполнение следующих мероприятий:

5.2.1. в случае использования единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным

биометрическим персональным данным гражданина Российской Федерации, - реализацию технических и организационных мер[1] в целях нейтрализации угроз безопасности, актуальных при обработке, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации;

5.2.2. в случае использования единой системы идентификации и аутентификации - соблюдение требований к обеспечению защиты информации в соответствии с Техническими требованиями к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия[2].

Указанная технология обработки защищаемой информации распространяется в том числе на идентификацию Потребителей финансовых услуг в соответствии с Федеральным законом от 07.08.2001 №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и аутентификацию участников Финансовой платформы при заключении и исполнении Финансовых сделок.

5.3. Технология обработки защищаемой информации, применяемая при формировании (подготовке), передаче и приёме Электронных сообщений, должна обеспечивать выполнение следующих мероприятий:

5.3.1. проверку правильности формирования (подготовки) Электронных сообщений (двойной контроль);

5.3.2. проверку правильности заполнения полей Электронного сообщения и прав владельца электронной подписи (входной контроль);

5.3.3. контроль дублирования Электронного сообщения;

5.3.4. структурный контроль Электронных сообщений;

5.3.5. защиту, в том числе криптографическую, защищаемой информации при ее передаче по каналам связи.

5.4. Технология обработки защищаемой информации, применяемая при удостоверении права Потребителя финансовых услуг Общества распоряжаться денежными средствами, должна обеспечивать выполнение следующих мероприятий:

5.4.1. получение Электронных сообщений Потребителя финансовых услуг, подписанных им способом, позволяющим обеспечить целостность подписываемых документов и подтвердить их составление уполномоченным на это лицом;

5.4.2. получение от Потребителя финансовых услуг подтверждения совершаемой финансовой сделки.

[1] В соответствии с приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 №21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" и приказом Федеральной службы безопасности Российской Федерации от 10.07.2014 №378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности".

[2] Утверждены приказом Министерства связи и массовых коммуникаций Российской Федерации от 23.06.2015 №210 "Об утверждении Технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия", зарегистрированным Министерством юстиции Российской Федерации 25.08.2015 №38668, 02.06.2017 №46934.

5.5. Технология обработки защищаемой информации, применяемая при осуществлении финансовой операции, учёте результатов её осуществления (при наличии учёта), должна обеспечивать выполнение следующих мероприятий:
5.5.1. проверку соответствия (сверку) выходных Электронных сообщений соответствующим входным Электронным сообщениям;
5.5.2. проверку соответствия (сверку) результатов осуществления финансовых сделок информации, содержащейся в Электронных сообщениях;
5.5.3. направление Потребителям финансовых услуг Общества уведомлений об осуществлении финансовых сделок в случае, когда такое уведомление предусмотрено законодательством Российской Федерации, нормативными актами, регулирующим деятельность Общества, или договором.
5.6. Общество должно реализовывать механизмы подтверждения принадлежности Потребителю финансовых услуг адреса электронной почты, на который Обществом направляются уведомления о совершаемых финансовых сделках, в том числе при предоставлении Потребителю финансовых услуг справок (выписок) по финансовым сделкам.

6. ИНЦИДЕНТЫ ЗАЩИТЫ ИНФОРМАЦИИ

6.1. К инцидентам защиты информации относятся события, которые привели или могут привести к осуществлению финансовых сделок без согласия (волеизъявления) Потребителя финансовых услуг Общества, неоказанию услуг, связанных с осуществлением финансовых сделок, в том числе события, включённые в перечень типов инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и размещаемый Банком России на своем официальном сайте в информационно-телекоммуникационной сети «Интернет».

6.2. По каждому Инциденту защиты информации Общество должно осуществлять регистрацию:
6.2.1. защищаемой информации на Технологических участках, на которых произошел несанкционированный доступ к защищаемой информации;
6.2.2. результата реагирования на Инцидент защиты информации, в том числе совершенных действий по возврату денежных средств Потребителя финансовых услуг Общества.

6.3. Общество должно информировать Банк России:
6.3.1. о выявленных Инцидентах защиты информации, включенных в перечень типов инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и размещаемый Банком России на своем официальном сайте в информационно-телекоммуникационной сети «Интернет», включая следующие:
6.3.1.1. получение Обществом от Потребителя финансовых услуг уведомления о списании денежных средств со Специального счёта без волеизъявления Потребителя финансовых услуг;

6.3.1.2. выявление Обществом в рамках реализуемой им системы управления рисками случаев и/или попыток совершения операций по списанию денежных средств со Специального счёта без волеизъявления Потребителя финансовых услуг, в том числе совершённых в результате несанкционированного доступа к объектам информационной инфраструктуры Общества;
6.3.1.3. получение Обществом от участников Финансовой платформы уведомлений о случаях и(или) попытках совершения операций по финансовым сделкам без волеизъявления участников финансовой платформы, кроме события, предусмотренного пунктом 6.3.1.1;
6.3.1.4. выявление Обществом случаев и/или попыток совершения операций по финансовым сделкам без волеизъявления участников Финансовой платформы, совершённых в результате несанкционированного доступа к объектам информационной инфраструктуры Общества, кроме события, предусмотренного пунктом 6.3.1.2;
6.3.1.5. выявление Обществом компьютерных атак, направленных на объекты информационной инфраструктуры Общества и(или) участников Финансовой платформы, которые могут привести к случаям и(или) попыткам осуществления операций по финансовым сделкам без волеизъявления участников Финансовой платформы, а также о принятых мерах и проведённых мероприятиях по реагированию на выявленный Обществом или Банком России Инцидент защиты информации;
6.3.1.6. о принадлежащих Обществу и(или) администрируемых в его интересах сайтах в информационно-телекоммуникационной сети «Интернет», используемых Обществом для осуществления деятельности Оператора финансовой платформы;
6.3.1.7. о планируемых мероприятиях, включая выпуск пресс-релизов и проведение пресс-конференций, размещение информации на официальных сайтах в информационно-телекоммуникационной сети «Интернет», в отношении Инцидентов защиты информации не позднее 1 (одного) рабочего дня до дня проведения мероприятия.

6.4. Общество предоставляет в Банк России сведения, указанные в пункте 6.3 Правил, с использованием технической инфраструктуры (автоматизированной системы) Банка России, а в случае технической невозможности такого взаимодействия - с использованием резервного способа взаимодействия, сведения о котором размещены на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет». Информация обо всех случаях и (или) о попытках осуществления операций по финансовым сделкам без волеизъявления участников Финансовой платформы, направленная с использованием резервного способа взаимодействия, должна быть повторно направлена Операторами финансовых платформ в Банк России с использованием технической инфраструктуры (автоматизированной системы) Банка России при возобновлении технической возможности взаимодействия Операторов финансовых платформ с Банком России.

6.5. Порядок, сроки, содержание направляемых в соответствии с пунктом 6.3 Правил сообщений регулируются Указанием Банка России от 15.12.2020 №5662-У.

7. ВЫЯВЛЕНИЕ И ПРОТИВОДЕЙСТВИЕ ОСУЩЕСТВЛЕНИЮ ОПЕРАЦИЙ, НАПРАВЛЕННЫХ НА СОВЕРШЕНИЕ ФИНАНСОВЫХ СДЕЛОК С ИСПОЛЬЗОВАНИЕМ ФИНАНСОВОЙ ПЛАТФОРМЫ БЕЗ ВОЛЕИЗЪЯВЛЕНИЯ УЧАСТНИКОВ ФИНАНСОВОЙ ПЛАТФОРМЫ

7.1. Общество создает и использует систему выявления и мониторинга случаев и(или) попыток совершения операций по финансовым сделкам без волеизъявления участников финансовой платформы (далее - Сделки без волеизъявления) в рамках реализуемой им системы управления рисками, в том числе на основании информации, полученной из базы данных, в рамках которой Общество:

7.1.1. выявляет случаи и(или) попытки совершения Сделок без волеизъявления, в том числе совершенные в результате несанкционированного доступа к объектам информационной инфраструктуры Общества;

7.1.2. при наличии подозрений о совершении операции по списанию денежных средств Потребителя финансовых услуг со Специального счета без волеизъявления Потребителя финансовых услуг, Оператор финансовой платформы должен получить дополнительное подтверждение от Потребителя финансовых услуг;

7.1.3. применяет полученную от Банка России информацию, содержащуюся в базе данных, в целях выявления случаев и(или) попыток совершения Сделок без волеизъявления;

7.1.4. выявляет компьютерные атаки, направленные на объекты информационной инфраструктуры Общества и(или) участников Финансовой платформы, которые могут привести к случаям и(или) попыткам осуществления Сделок без волеизъявления;

7.1.5. осуществляет сбор технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры Общества и(или) участников финансовой платформы (при их наличии);

7.1.6. реализовывает меры по выявлению и устранению причин и последствий компьютерных атак, направленных на объекты информационной инфраструктуры Общества и(или) участников финансовой платформы, и дальнейшему предотвращению случаев и(или) попыток осуществления Сделок без волеизъявления;

7.1.7. реализовывает условия для направления участниками Финансовой платформы уведомлений о случаях и(или) попытках совершения Сделок без волеизъявления, а также обеспечивает учет, регистрацию и хранение указанных уведомлений на срок не менее 5 (пяти) лет с даты их поступления;

7.1.8. при выявлении/получении информации о технических данных, описывающих компьютерные атаки, направленные на информационную инфраструктуру Общества и/или участников Финансовой платформы, Общество должно осуществлять мероприятия по противодействию осуществлению Сделок без волеизъявления в соответствии с требованиями ГОСТ Р 57580.1-2017;

7.1.9. обеспечивает для показателя, характеризующего уровень Сделок без волеизъявления, на ежеквартальной основе значение не более 0,005%[3] в рамках применения

[3] Значение показателя, характеризующего уровень финансовых сделок без волеизъявления участников финансовой платформы, должно рассчитываться как отношение суммы денежных средств, в отношении которых от участников финансовой платформы получены уведомления об осуществлении Сделок без волеизъявления, повлекших списание денежных средств со Специального счета без их волеизъявления, за оцениваемый квартал (за исключением случаев, предусмотренных законодательством Российской Федерации) к общей сумме денежных средств по финансовым сделкам.

Обществом мер защиты информации, а также ограничений по параметрам операций по Финансовым сделкам, устанавливаемых на основании заявления участника Финансовой платформы, переданного способом, определенным в договоре Общества с участником Финансовой платформы.

7.2. Общество на основании договора, заключенного между ним и кредитной организацией, в которой обслуживается Специальный счет Общества, вправе привлечь кредитную организацию для выявления случаев и(или) попыток совершения Сделок без волеизъявления.

7.3. Общество должно в порядке, установленном им во внутренних документах, вести учет фактов обращений участников Финансовой платформы в правоохранительные органы в связи со случаями и(или) попытками совершения Сделок без волеизъявления при поступлении от участников Финансовой платформы информации о таких обращениях.

8. РЕАЛИЗАЦИЯ ОБЩЕСТВОМ СТАНДАРТНОГО УРОВНЯ ЗАЩИТЫ ИНФОРМАЦИИ

8.1. Если Общество реализует стандартный уровень защиты информации, то дополнительно Общество должно:

8.1.1. осуществлять ежегодное тестирование объектов информационной инфраструктуры на предмет проникновений и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры;

8.1.2. в случае выявления уязвимостей информационной безопасности объектов информационной инфраструктуры, устранять выявленные уязвимости в порядке и сроки, установленные во внутренних документах Общества;

8.1.3. обеспечить использование для осуществления финансовых сделок (операций) прикладного программного обеспечения, автоматизированных систем и приложений, распространяемых Обществом Потребителям для совершения действий в целях осуществления финансовых сделок (операций), а также программного обеспечения, обрабатывающего защищаемую информацию при приёме Электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети «Интернет», прошедших сертификацию не ниже 5 уровня доверия или оценку соответствия в соответствии с требованиями законодательства Российской Федерации. В отношении иного программного обеспечения и приложений Общество должно самостоятельно определять необходимость их сертификации или оценки соответствия;

8.1.4. обеспечить целостность Электронных сообщений и подтвердить их составление уполномоченным на это лицом;

8.1.5. в соответствии с пунктом 8.2 Правил обеспечить регистрацию результатов выполнения действий, связанных с осуществлением доступа к защищаемой информации, на всех Технологических участках, включая регистрацию действий своих работников и Потребителей, выполняемых с использованием автоматизированных систем, программного обеспечения;

8.1.6. обеспечить хранение информации, указанной в пунктах 1.2.1 и 1.2.3 Правил, информации о регистрации данных, указанных в пункте 8.2 Правил, и информации об инцидентах, связанных с обеспечением защиты информации при осуществлении деятельности в сфере финансовых рынков, а также целостность и доступность такой информации в течение не менее 5 (пяти) лет с даты ее формирования Обществом (даты поступления в Общество) или в течение иного срока, предусмотренного законодательством Российской Федерации;

8.2. Общество регистрирует следующую информацию о действиях своих работников, Потребителей, выполняемых с использованием автоматизированных систем, программного обеспечения:
8.2.1. в отношении работника - дату (день, месяц, год) и время (часы, минуты, секунды) осуществления финансовой операции, в отношении Потребителя - совершение действий в целях осуществления финансовой сделки (операции);
8.2.2. присвоенный работнику (Потребителю) идентификатор, позволяющий идентифицировать работника (Потребителя) в автоматизированной системе и(или) программном обеспечении;
8.2.3. код, соответствующий Технологическому участку;
8.2.4. в отношении работника - результат осуществления финансовой сделки (операции), а в отношении Потребителя - совершение действий в целях осуществления финансовой сделки (операции);
8.2.5. информацию, используемую для идентификации устройства, с применением которого осуществлен доступ к автоматизированной системе, программному обеспечению, с целью осуществления финансовых сделок (операций): сетевой адрес компьютера и/или коммуникационного устройства (маршрутизатора) работника (Потребителя), международный идентификатор абонента-Потребителя (индивидуальный номер абонента-Потребителя), международный идентификатор пользовательского оборудования (оконечного оборудования) Потребителя, номер телефона и/или иной идентификатор устройства Потребителя.

9. ПРАВИЛА РАСКРЫТИЯ ИНФОРМАЦИИ

9.1. Общество как Оператор финансовой платформы раскрывает на своем сайте в информационно-телекоммуникационной сети «Интернет» следующую информацию и документы:
9.1.1. фирменное наименование Общества, сведения о государственной регистрации юридического лица, сведения о регистрации Общества как оператора финансовой платформы в реестре операторов финансовых платформ;
9.1.2. место нахождения Общества;
9.1.3. устав Общества;
9.1.4. правила финансовой платформы и сведения об их регистрации в Банке России;
9.1.5. размер вознаграждения Общества как Оператора финансовой платформы или порядок его определения, порядок уплаты такого вознаграждения;
9.1.6. реквизиты Специального счета или счетов Оператора финансовой платформы (при наличии);

9.1.7. 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 (если применимо);
9.1.8. перечень лиц, привлекаемых Обществом 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;
9.1.9. перечень банков, которым Обществом как Оператором финансовой платформы поручено проведение идентификации Потребителей финансовых услуг при их личном присутствии, представителей Потребителей, выгодоприобретателей, бенефициарных владельцев в целях заключения с такими Потребителями договора об оказании услуг Оператора финансовой платформы;
9.1.10. сведения о выявленных конфликтах интересов и принятых мерах по минимизации риска их негативных последствий;
9.1.11. информация о технических сбоях в функционировании программно-аппаратных средств, необходимых для оказания услуг 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;
9.1.12. фирменные наименования и места нахождения Финансовых организаций и эмитентов (если применимо), являющихся участниками финансовой платформы или указатели страниц сайтов таких финансовых организаций и таких эмитентов в информационно-телекоммуникационной сети «Интернет» или сетевых адресов, позволяющих идентифицировать их сайты в информационно-телекоммуникационной сети «Интернет»;
9.1.13. информация о расторжении договора об оказании услуг Оператора финансовой платформы между Оператором финансовой платформы и Финансовой организацией или эмитентом и о последствиях расторжения такого договора;
9.1.14. иная информация в случае, если требование о ее раскрытии установлено Банком России.

ИЗМЕНЕНИЯ

Номер редакции	Дата изменений	Описание изменений
1	05.09.2023	Документ введен впервые.