Комплекс мер безопасности при работе с электронной платформой «ФИНФЭКТОРИ»

(далее – Платформа)

1. Для целей настоящего документа использованные в нем термины соответствуют терминам и определениям, указанным в Регламенте подключения и использования электронной платформы «ФИНФЭКТОРИ», утвержденном Приказом Генерального директора ООО «Финфэктори» № 2 от 01.07.2025 года, если иное специально не оговорено в настоящем документе, а также используются в том значении, в котором они определены законодательством Российской Федерации.

2. Общие требования по обеспечению информационной безопасности: ООО «Финфэктори» (далее – Оператор Платформы) постоянно работает над повышением безопасности работы на Платформе, при этом максимально сохраняя удобство пользования услугами и продуктами Платформы.

Для защиты Участников Платформы и их уполномоченных лиц используются:

- шифрование канала связи с использованием протокола TLS 1.2;
- усиленные квалифицированные электронные подписи (далее – КЭП) для подписания Электронных документов;
- регистрация и аутентификация Участника (пользователя) Платформы по логину и паролю
- ключевые носители (токены) для генерации, надежного хранения и безопасной работы с КЭП.

3. Участники и Пользователи Платформы обязаны соблюдать требования по обеспечению информационной безопасности при обмене Электронными документами на Платформе, предусмотренные законодательством Российской Федерации и настоящим документом, а также соблюдать требования по обеспечению безопасности использования усиленной квалифицированной электронной подписи и средств КЭП.

4. Для обеспечения целостности, конфиденциальности и подтверждения авторства информации, передаваемой в рамках Платформы, на рабочем месте Уполномоченного лица Участника Платформы должны быть установлены средства криптографической защиты информации (СКЗИ) и передаваемая информация должна подписываться усиленной квалифицированной электронной подписью.

Порядок обеспечения информационной безопасности при работе на Платформе определяется Участником на основе требований и рекомендаций по организационно-техническим мерам защиты, изложенным в настоящем документе, эксплуатационной документации на СКЗИ, а также требований действующего российского законодательства в области защиты информации.

5. Участник и Пользователи Платформы должны четко соблюдать требования руководства по обеспечению безопасности использования усиленной квалифицированной электронной подписи и средств квалифицированной электронной подписи, выданного удостоверяющим центром, в котором выдан соответствующий квалифицированный сертификат проверки электронной подписи, в том числе, но, не ограничиваясь:

- Пользователи (уполномоченные лица) участника Платформы, являющиеся владельцами квалифицированного сертификата ключа проверки КЭП, обязаны:
- обеспечить конфиденциальность КЭП;

- применять для формирования электронной подписи только КЭП, соответствующий действующему сертификату ключа проверки электронной подписи;
- не применять КЭП при наличии оснований полагать, что конфиденциальность данного КЭП нарушена;
- незамедлительно сообщить Оператору Платформы и обратиться в удостоверяющий центр в случае нарушения конфиденциальности или подозрения в нарушении конфиденциальности КЭП;
- не использовать КЭП, связанный с сертификатом ключа проверки электронной подписи, заявление на блокировку/аннулирование которого подано в удостоверяющий центр, выдавший указанный сертификат;
- использовать для создания и проверки усиленной квалифицированной электронной подписи, создания ЭП и ключей проверки электронной подписи, сертифицированные в соответствии с правилами сертификации Российской Федерации средства электронной подписи, в том числе выданные удостоверяющим центром.

6. При использовании средств КЭП Пользователи (уполномоченные лица Участника), являющие владельцами квалифицированного сертификата ключа проверки электронной подписи, обязаны:

- руководствоваться положениями эксплуатационной документации на применяемое средство усиленной квалифицированной электронной подписи, предоставленной удостоверяющим центром и/или производителем, в том числе не разглашать содержимое носителей ключевой информации и не передавать сами носители лицам, к ним не допущенным, не выводить ключевую информацию (информацию закрытого ключа) на экран компьютера (дисплей), принтер и иные средства отображения информации, не копировать ключевую информацию на иные носители, не записывать на ключевые носители постороннюю информацию, совершать прочие действия ведущие к нарушению целостности конфиденциальности ключевой информации;
- хранить ключевые носители, эксплуатационную и техническую документацию, инсталлирующие средства квалифицированной электронной подписи в запираемых шкафах (ящиках, сейфах) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у владельцев средств квалифицированной электронной подписи.

7. Обеспечение информационной безопасности на рабочем месте Пользователя (уполномоченного лица) Участника Платформы:

7.1. Для повышения безопасности при работе на Платформе необходимо следовать следующим рекомендациям:

- разработать нормативные документы, регламентирующие вопросы обеспечения информационной безопасности, в том числе безопасности при эксплуатации средств квалифицированной электронной подписи.
- назначить должностных лиц, ответственных за обеспечение безопасности информации и эксплуатации средств квалифицированной электронной подписи при работе на Платформе.
- определить и утвердить список лиц, имеющих персонифицированный доступ к ключевой информации. Не допускать доступа лиц к ключевой информации других пользователей.

- вести учет средств квалифицированной электронной подписи и ключевых носителей в соответствии с их серийными номерами.
- не хранить КЭП на жестком диске компьютера. Использовать сертифицированные ключевые носители (токены) для хранения КЭП. Использование ключевых носителей значительно повышает сохранность КЭП. Хранить ключевые носители в недоступном для посторонних месте (сейфы, закрываемые ящики).
- ни при каких условиях не передавать носители и не сообщать информацию о пароле к КЭП никому, включая сотрудников Оператора Платформы, родственников, сотрудников Участника Платформы (в том числе руководителей) и иных третьих лиц. Не хранить информацию о пароле от ЭП на любых носителях, включая жесткий диск компьютера. Если возникли подозрения, что кто-либо владеет информацией о пароле от КЭП, необходимо немедленно обратиться в удостоверяющий центр и потребовать отзыв сертификата ключа проверки электронной подписи или аннулирования сертификата, соответственно.

  В случае увольнения Уполномоченного лица Участника, иного сотрудника, имевшего доступ к Платформе, немедленно произвести блокировку такого Пользователя на Платформе, сообщить Оператору Платформы об увольнении Пользователя и отзыве его доверенности, а также обратится в удостоверяющий центр с заявлением на аннулирование сертификата ключа проверки электронной подписи.
- ни в коем случае не сообщать никому личный пароль для входа на Платформу. Не хранить информацию о пароле для входа в личный кабинет участника на Платформе на любых носителях, включая жесткий диск компьютера. Если возникли подозрения, что кто-либо владеет информацией о пароле для входа на Платформу, то Участнику/Пользователю необходимо незамедлительно самостоятельно сменить пароль для входа на Платформу и уведомить о возникновении такой ситуации Оператора Платформы.
- своевременно производить замену сертификата ключа проверки электронной подписи по истечении срока его действия и в соответствии с установленным удостоверяющим центром регламентом.
- в случае изменения у Пользователей (уполномоченных лиц) Участника имени, фамилии, отчества, полномочий или лишения их права работы на Платформе немедленно сообщить Оператору Платформы и в Удостоверяющий центр.
- не держать носители с КЭП постоянно вставленными в компьютер, использовать их только при необходимости подписания документов на Платформе. Не оставлять компьютер при включенном питании, загруженном программном обеспечении СКЗИ после ввода ключевой информации и с активным входом на Платформу без присмотра. При уходе с рабочего места, даже если необходимо отойти на непродолжительное время, выходить из личного кабинета Платформы или блокировать рабочее место (блокировка, защищенная паролем), либо использовать иные дополнительные организационно-режимные меры, исключающие несанкционированный доступ к рабочему месту. После окончания работы в личному кабинете Участника на Платформе

обязательно закрыть окно личного кабинета Участника с помощью кнопки «ВЫХОД». После выхода необходимо обязательно извлечь из компьютера ключевой носитель, на котором хранится КЭП;

- ограничить доступ сотрудников Участников и посторонних лиц к КЭП и компьютерам с установленными СКЗИ, с которых осуществляется работа на Платформе и обеспечить контроль за их действиями. Рекомендуется использовать рабочие места с СКЗИ в однопользовательском режиме. При использовании рабочего места с СКЗИ несколькими Уполномоченными лицами Участника, эти лица должны обладать равными правами доступа к личному кабинету Участника на Платформе.
- рекомендуется использовать в пароле символы следующих четырех категорий:
  - ✓ прописные буквы в европейских языках (от A до Z, от А до Я),
  - ✓ строчные буквы европейских языков (от a до z, от а до я),
  - ✓ десятичные цифры (от 0 до 9),
  - ✓ символы, отличные от алфавитно-цифровых (специальные знаки): (~! @ # $% ^& * - + = ' |{}\ \ () \ []:; " <>,.? /).
- убедиться, что используемый компьютер не заражен вирусами, запустив проверку компьютера антивирусным программным обеспечением. Для предотвращения заражения компьютера с установленными средствами квалифицированной электронной подписи, с которого осуществляется работа на Платформе, необходимо обеспечить непрерывную комплексную защиту компьютера от вирусов, хакерских атак и других вредоносных программ, установив и активизировав антивирусное программное обеспечение. Необходимо регулярно обновлять антивирусные базы (действие вирусов может быть направлено, в том числе на запоминание и передачу третьим лицам информации о пароле и КЭП).
- Осуществлять контроль над отправляемыми Электронными документами при работе на Платформе.
- не работать в личном кабинете Участника на Платформе с гостевых рабочих мест и иных, не проверенных компьютеров (Интернет-кафе, киоски), а также терминальных серверов общего доступа.
- при каждом сеансе работы на Платформе, проверять подлинность соединения.
- Убедиться, что используемый информационный ресурс не является ложным (фальсифицированным), для чего необходимо удостовериться, что соединение установлено именно с сервером Оператора Платформы, т.е. в адресной строке Интернет - страницы указан точный адрес: https://finfactory.one. Убедиться, что канал связи с Платформой защищен, и доступ осуществляется по протоколу https (при незащищенном соединении буквы https в адресной строке браузера будут перечеркнуты). Обращайте внимание на изменения привычных процессов входа или функционирования Платформы. Если есть сомнения в правильности функционирования Платформы, необходимо обязательно связаться с Оператором Платформы.
- установить и настроить персональный межсетевой экран (firewall) на компьютере, на котором осуществляется работа с Платформой. При

наличии возможности ограничить на сетевом оборудовании (межсетевые экраны, маршрутизаторы) взаимодействие компьютера (на котором осуществляется работа с Платформой) с сетью Интернет только адресами Платформы.

- не устанавливать на компьютере, на котором осуществляется работа с Платформой, программное обеспечение удаленного управления, в том числе TeamVeiwer, RAdmin, VNC и иное подобное программное обеспечение.
- использовать лицензионное программное обеспечение из проверенных и надежных источников. Выполнять регулярные обновления операционной системы и прикладного программного обеспечения (браузер, программы для работы с документами).
- при обнаружении попыток несанкционированного доступа или в случае мотивированных опасений, что такие попытки могут быть осуществлены, в том числе при обнаружении подозрительной активности на компьютере, с которого осуществляется работа на Платформе (самопроизвольные движения мышью, открытие/закрытие окон, набор текста), мошеннических действий в отношении Участника и т.д., необходимо немедленно:
  - ✓ сообщить Оператору Платформы о возможной попытке несанкционированного доступа к Платформе;
  - ✓ сверить последние подписанные и отправленные Электронные документы, при обнаружении несанкционированных Электронных документов поставьте в известность Участника(ов) – получателя(ей) указанных документов, и Оператора Платформы;
  - ✓ блокировать технические средства (в том числе, выключите компьютер используя «гибернацию» или «завершение работы»), используемые для работы на Платформе;
  - ✓ предпринять меры по сохранению лог файла работы в сети Интернет (данные с прокси- сервера, брандмауэра клиента);
  - ✓ предоставить Оператору Платформы и Участнику - получателю несанкционированных Электронных документов письменное описание обстоятельств компрометации ключей или несанкционированного доступа.

При возникновении дополнительных вопросов рекомендуется обращаться к Оператору Платформы по номерам телефонов 8-985-970-40-79 или электронному адресу support@finfactory.one.