

Соглашение об обеспечении информационной безопасности

Соглашение об обеспечении информационной безопасности (далее – Соглашение) устанавливает требования и рекомендации, предъявляемые ПАО «Самараэнерго» (далее - Общество) к третьим лицам/поставщикам/подрядчикам (далее каждый по отдельности — Подрядчик) и необходимые для обеспечения информационной безопасности и защиты интересов Общества при использовании Подрядчиками информационных активов Общества. Настоящее Соглашение применимо ко всем Подрядчикам и их субподрядчикам, которые хранят, обрабатывают или имеют доступ к данным Общества. Требования настоящего Соглашения в обязательном порядке учитываются при заключении договоров с Подрядчиками, которые хранят, обрабатывают или имеют доступ к данным, информационной инфраструктуре и/или информационным системам Общества.

Любые дополнительные обязательства Подрядчика в отношении информационной безопасности по любому соглашению с Обществом являются дополнением к требованиям, изложенным в настоящем Соглашении.

В контексте настоящего Соглашения термин «Информация» включает Конфиденциальную информацию, используемую в процессе осуществления коммерческой деятельности (далее — «Информация»). Конфиденциальная информация — это любая информация (сведения, сообщения, данные) о лицах, предметах, фактах, событиях, явлениях и процессах, обозначенная Обществом в качестве Конфиденциальной информации и переданная в соответствии с порядком, указанным в Соглашении о конфиденциальности, которое должно оформляться соответствующим приложением к договору.

Настоящим поясняется, что данное Соглашение применимо ко всей Информации, обрабатываемой Подрядчиком, в том числе, обрабатываемой при:

1. Создании;
2. Редактировании;
3. Управлении;
4. Получении доступа;
5. Получении;
6. Передаче;
7. Уничтожении;
8. Хранении или размещении на сервере в любом формате, в том числе в системах и ресурсах, находящихся в памяти средств вычислительной техники, на электронных устройствах и версии такой Информации на неэлектронных носителях.

Общество в праве запрашивать у Подрядчика сведения о применяемых Подрядчиком политик, процессов и процедур по обеспечению информационной безопасности (физической безопасности, конфиденциальности Информации, политики информационной безопасности, результаты тестирования на проникновение, результаты аудита по информационной безопасности, план реагирования на компьютерные инциденты, регламент работников Подрядчика в случае нештатной ситуации и т.п.).

Общество вправе приостановить доступ к Информации Общества работнику Подрядчика в случае нарушения им требований настоящего Соглашения.

1. Общие сведения

ПАО «Самараэнерго» в соответствии с Федеральным законом от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» является субъектом критической информационной инфраструктуры Российской Федерации. Информационные системы Общества, в соответствии с Федеральным законом от 26.07.2017 №187-ФЗ, являются объектами критической информационной инфраструктуры Российской Федерации (далее – ОКИИ).

2. Законодательные нормативные акты

Обеспечение информационной безопасности ОКИИ ПАО «Самараэнерго» реализуется в соответствии с действующими законодательными правовыми актами по информационной безопасности и безопасности критической информационной инфраструктуры РФ, в том числе:

- Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года №187-ФЗ;
- Приказ ФСТЭК России от 25 декабря 2017 года № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
- Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».
- Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ.

Подрядчик уведомлен о том, что в соответствии со статьей 274.1 Уголовного Кодекса Российской Федерации предусмотрена уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации:

Ч.1. Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации,

- наказываются принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода, осужденного за период от одного года до трех лет.

Ч.2. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации,

- наказывается принудительными работами на срок до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода, осужденного за период от одного года до трех лет и с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до шести лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода, осужденного за период от одного года до трех лет.

Ч.3. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации,

- наказывается принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового либо лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Ч.4. Деяния, предусмотренные частью первой, второй или третьей настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения,

- наказываются лишением свободы на срок от трех до восьми лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Ч.5. Деяния, предусмотренные частью первой, второй, третьей или четвертой настоящей статьи, если они повлекли тяжкие последствия,

- наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

3. Правила и процедуры обеспечения информационной безопасности

Подрядчик должен принять и соблюдать настоящее Соглашение и процедуры в отношении информационной безопасности в целях создания контролируемой среды (далее - Среда), связанной с защитой конфиденциальности, целостности и доступности информации Общества.

Подрядчик должен обеспечить подписание работниками Подрядчика, до начала работ по договору, обязательства о неразглашении сведений конфиденциального характера и соблюдения требований по защите информации в соответствии с настоящим Соглашением (далее – Обязательство).

Подрядчик должен обеспечить проведение инструктажа работников Подрядчика требованиям по информационной безопасности и защите персональных данных, действующих в Обществе, до начала работ по договору, и передать оригиналы журнала инструктажа с подписями указанных работников в течение 10 рабочих дней после подписания путем направления заказным письмом с уведомлением о вручении или передачи уполномоченному работнику Общества, согласно Приложению №1 к настоящему Соглашению.

При получении от Общества информации о внесении изменений в настоящее Соглашение, Подрядчик должен довести такие изменения до своих работников и субподрядчиков, выполняющих работы по договорам, заключенным с Обществом под подпись.

Доступ работникам Подрядчика для работы с Информацией Общества предоставляется только после получения Обществом оригиналов журнала инструктажа, подписанных работниками Подрядчика.

При заключении договора Подрядчик обязуется определить своего представителя в качестве единственного контактного лица по всем вопросам, связанным с информационной безопасностью. В дополнение Подрядчик должен определить представителя, ответственного за контроль соблюдения настоящего Соглашения.

4. Правила безопасной эксплуатации ОКИИ

При производстве работ с ОКИИ Общества персоналу Подрядчика, запрещается:

- использовать компоненты программного и аппаратного обеспечения ОКИИ в целях, не связанных с исполнением договора;
- самостоятельно производить сборку, разборку, установку и техническое обслуживание аппаратных средств, а также допускать проведение таких работ другими лицами (кроме лиц, уполномоченных на производство таких работ);
- самостоятельно вносить какие-либо изменения в конфигурацию программно-аппаратных средств или устанавливать дополнительно любые программные и аппаратные средства, а также допускать проведение таких работ другими лицами (кроме лиц, уполномоченных на производство таких работ);
- самостоятельно создавать сетевые ресурсы или организовывать сетевые сервисы (общие сетевые диски, прокси- или веб-серверы, Wi-Fi точки доступа и т. д., кроме лиц, уполномоченных на производство таких работ);
- использовать неучтенные машинные носители информации;
- передавать свои реквизиты доступа (логин, пароль) для использования другим лицам;
- использовать персональные реквизиты доступа других лиц, а также связанные с ними права доступа и функциональные возможности;
- оставлять без личного присмотра в местах, доступных другим лицам, свои реквизиты доступа, машинные и бумажные носители, содержащие конфиденциальную информацию;
- самостоятельно изменять, без письменного согласования, параметры и настройки программного обеспечения ОКИИ;
- загружать в средства вычислительной техники ПАО «Самараэнерго» информацию, доступ к которой ограничен законодательством Российской Федерации и не относящуюся к исполнению договора;
- осуществлять попытки и поиск способов обхода, удаления или преодоления установленных программных и аппаратно-программных средств защиты информации;
- посещать сайты сети «Интернет» и загружать web-трафик в средства вычислительной техники ПАО «Самараэнерго» не связанными с исполнением договора;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты информации, которые могут привести к ознакомлению с конфиденциальной информацией посторонних лиц или к предоставлению доступа к ОКИИ посторонних лиц;
- производить перемещения технических средств ОКИИ без согласования с представителем Общества;
- выносить/вносить компоненты ОКИИ, материальные носители и прочее имущество ПАО «Самараэнерго» за пределы контролируемой зоны без согласования с представителем Общества;
- нарушать правила эксплуатации программного обеспечения и оборудования ОКИИ.
- использовать программное обеспечение для удаленного управления рабочим местом (например: TeamViewer, AnyDesk, AmmyAdmin, AeroAdmin, Radmin, LiteManager, Chrome, Microsoft Remote Assistance и Desktop).

5. Доступ к Информации

Подрядчик должен обеспечивать, как минимум, следующие меры контроля при работе с учетными записями, когда Подрядчик обладает Информацией, принадлежащей или доверенной Обществом и находящейся за пределами Среды Общества, и (или) когда Подрядчик устанавливает удаленное подключение к Среде Общества:

1. Процесс предоставления доступа осуществлялся, исходя из рабочей потребности по выполнению должностных обязанностей (т.е. наделение минимальным объемом полномочий, исключительно исходя из необходимого уровня доступа).
2. В случае необходимости получения удаленного доступа к информационной инфраструктуре Общества, Подрядчик должен направить на согласование официальный запрос, содержащий список сотрудников Подрядчика, которым требуется получение удаленного доступа, в соответствии с формой, указанной в Договоре.
3. Учетные записи для доступа к системам и приложениям должны закрепляться за каждым отдельным пользователем и быть уникальными, а не являться общими.
4. Работники Подрядчика должны иметь уникальный идентификатор, позволяющий однозначно определить работника и организацию.
5. Работники Подрядчика должны осуществлять работы по договору в рабочее время Общества (с 8:00 до 17:00, с понедельника по пятницу, за исключением праздничных дней, установленных Российской Федерации). В случае необходимости осуществлять работы в не рабочее время, такой доступ требуется согласовать с Обществом, направив официальное письмо.
6. В ОКИИ установлены следующие требования к аутентификационной информации, при наличии технической возможности, предусмотренной производителем программных и аппаратных средств:
 - длина пароля должна быть не менее 12 символов для пользовательских учетных записей;
 - длина пароля для пользовательской учетной записи не менее 12 символов;
 - длина пароля администратора учетной записи не менее 15 символов;
 - пароль не должен содержать: имя, фамилию, дату рождения, месяц, логин, название организации;
 - пароль должен содержать латинские заглавные буквы (от А до Z);
 - пароль должен содержать латинские строчные буквы (от а до z);
 - пароль должен содержать цифры (от 0 до 9);
 - пароль должен содержать отличающиеся от букв и цифр спецсимволы, например: !, \$, #, %;
 - пароль не должен содержать символы кириллицы;
 - пароль не должен содержать более 2 следующих друг за другом одинаковых символов.
 - пароль не должен содержать информацию личностного характера (например: имя, фамилию, дату рождения, месяц, логин, название организации в любых словоформах), а также основываться на словах естественного языка.
 - набор используемых символов для пароля должен состоять из букв в верхнем и нижнем регистрах, цифр и/или специальных символов (@, #, \$, &, *, % и т.п.), если это допускается производителем;
 - смена паролей производится не реже чем через 90 дней;
 - при смене пароля новое значение должно отличаться от предыдущего не менее чем в шести позициях.
 - в случае генерации паролей использовать псевдослучайные последовательности.
7. Работникам Подрядчика не допускается: хранить пароли в записанном виде таким образом, чтобы они были доступны посторонним лицам; хранить пароли в открытом виде в средстве вычислительной техники; размещать пароли на ресурсах общего доступа

или пересылать их по электронной почте в открытом виде; сообщать пароли посторонним лицам; применять пароли, используемые для аутентификации в ОКИИ, для доступа к иным системам; применять одинаковые пароли для различных учетных записей.

8. В случаях создания учетной записи к ОКИИ, персонал Подрядчика должен передать идентификационные и аутентификационные данные представителю Общества способом, обеспечивающим безопасность передаваемой информации.
9. В случае изменений в составе персонала Подрядчика, если сотрудники Подрядчика имеют учетные записи или им предоставлен доступ к информационным системам Общества, обеспечить направление уведомления в Общество о фактах таких изменений в течение 24 часов.
10. В случае увольнения сотрудника Подрядчика, имеющего доступ к информационным ресурсам Общества и/или технической информации по организации удаленного доступа к инфраструктуре Общества, а также при подозрении на компрометацию данных используемых для доступа к ресурсам Общества, Подрядчик должен обеспечить в максимально возможный короткий срок смену паролей всех сотрудников Подрядчика имеющих доступ к инфраструктуре Общества.

6. Сетевая и системная безопасность

Подрядчик должен применять, как минимум, следующие меры сетевой и системной безопасности, когда Подрядчик обладает Информацией, принадлежащей или доверенной Обществом и находящейся за пределами Среды Общества, и (или) когда Подрядчик устанавливает удаленное подключение к Среде Общества:

1. Осуществление обновления программного обеспечения и операционных систем до последней стабильной версии, в части установки «заплаток» или пакетов безопасности.
2. Техническое обслуживание систем Подрядчика должно осуществляться на уровне, позволяющем устанавливать последние обновления и внедрять сервисные пакеты безопасности.
3. Осуществление записи действий работников Подрядчика, хранение журналов событий.
4. Должна быть обеспечена антивирусная защита информации для автоматизированных рабочих мест работников и серверов Подрядчика.
5. Должно быть организовано и осуществлено защищенное удаленное подключение с использованием средств криптографической защиты информации.
6. Должна быть организована и осуществлена защита почтовых сервисов Подрядчика от «фишинга».
7. Должен быть организован и осуществлен защищенный обмен файлами и информацией через файловое хранилище.
8. При организации сетевых подключений к инфраструктуре Общества Подрядчик должен использовать межсетевой экран, ограничивающий входящий и исходящий трафик, исходя из текущих потребностей.
9. Пользовательские устройства, автоматизированные рабочие места и сервера Подрядчика должны быть защищены паролем.
10. Для доступа к информационной инфраструктуре Общества должны использоваться средства вычислительной техники и автоматизированные рабочие места, которые не используются в личных целях и к которым применяются настоящие меры по информационной безопасности.

7. Управление угрозами и уязвимостями

Подрядчик должен проводить непрерывную оценку уязвимостей и своевременно исправлять проблемы, связанные с приложениями, операционными системами и прочими компонентами своей инфраструктуры.

8. Управление активами

Подрядчик должен обеспечивать проведение инвентаризации своих активов, включая системы/устройства и программное обеспечение, когда Подрядчик обладает Информацией, принадлежащей или доверенной Обществом и находящейся за пределами Среды Общества, и (или) когда у Подрядчика есть удаленное подключение к Среде Общества.

9. Обработка Информации

Подрядчик должен обеспечить отделение Информации от информации прочих клиентов, если у Подрядчика имеется Информация, принадлежащая или доверенная Обществом, находящаяся за пределами Среды Общества, и/или если у Подрядчика есть удаленный доступ к Среде Общества. Кроме того, Подрядчик должен быть способен составить описание прохождения Информации через его Среду.

Электронный обмен информацией между Обществом и Подрядчиком (в том числе по электронной почте, путем передачи файлов, через удаленное подключение и т. д.) должен быть защищен с помощью взаимно согласованных сервисов.

10. Физическая безопасность

Подрядчику необходимо разработать и применять процедуры, и физические средства контроля для защиты копий Информации на бумажных носителях и информационных систем (например, аппаратное обеспечение, программное обеспечение, документация и данные), если у Подрядчика имеется Информация, принадлежащая или доверенная Обществом, находящаяся за пределами Среды Общества, и/или если у Подрядчика есть удаленный доступ к Среде Общества.

Центры обработки данных должны находиться под физическим контролем, включая формальное управление доступом в зависимости от рабочих потребностей.

11. Хранение и уничтожение записей

Подрядчик должен хранить Информацию только в течение срока, установленного в соответствующем соглашении, кроме случаев, когда по закону требуется более длительное хранение.

При истечении срока действия договоренности Подрядчик должен вернуть и гарантированно удалить Информацию.

По запросу Общества, Подрядчик должен подтвердить, что Информация была удалена.

12. Управление инцидентами информационной безопасности

Подрядчик должен в полной мере сотрудничать с Обществом для прояснения ситуации, понимания ключевых причин и определения необходимых действий для устранения таких причин в случае фактического или предполагаемого инцидента, связанного с информационной безопасностью.

Подрядчик должен организовать и обеспечить процесс управления уязвимостями в информационной инфраструктуре Подрядчика.

Подрядчик должен организовать и осуществлять регулярный мониторинг, выявление и реагирование на события информационной безопасности в информационной инфраструктуре Подрядчика, а также уведомлять Общество о наступлении в ее информационной инфраструктуре компьютерных инцидентов, в течение 3 часов с момента выявления.

Подрядчик должен осуществлять регулярное (минимум раз в год) проведение тренировок по реагированию на компьютерные инциденты и нештатные ситуации в информационной инфраструктуре Подрядчика.

Персонал Подрядной организации обязан незамедлительно сообщать представителю Общества о следующих фактах:

- нарушения целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах;

- утери машинных носителей информации;
- компрометации аутентификационной информации или о подозрениях на их компрометацию;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств;
- некорректного функционирования установленных программных и технических средств, в том числе средств защиты информации;
- попыток несанкционированного доступа (или подозрений о таких попытках) к обрабатываемой информации,
- заражения вредоносным программным обеспечением или других фактах, свидетельствующих о компьютерной атаке;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию;
- выхода из строя или неустойчивого функционирования элементов, а также перебоев в системе электроснабжения и связи.

13. Управление субподрядчиками

Настоящее Соглашение информационной безопасности применяется ко всем субподрядчикам, используемым Подрядчиком, которые работают с Информацией, принадлежащей или доверенной Обществом и находящейся за пределами Среды Общества, и (или) когда Подрядчик устанавливает удаленное подключение к Среде Общества. Подрядчик несет ответственность за то, чтобы обеспечивать уведомление каждого субподрядчика о содержании Соглашения информационной безопасности и его соблюдение таким субподрядчиком.

Подрядчик и субподрядчики должны заключать официальные контракты, в которых описаны необходимые меры контроля, включая меры контроля за обеспечением конфиденциальности, доступности и целостности Информации, содержащие в том числе требования настоящего Соглашения.

Подрядчику необходимо проводить первоначальные и текущие оценки в целях обеспечения соблюдения субподрядчиками Соглашения.

Подрядчик должен информировать Общество и получать письменное одобрение перед использованием услуг субподрядчиков, которые либо намереваются работать с Информацией, либо будут иметь доступ к системам Подрядчика или Общества, в которых находятся Информация, а также уведомлять Общество о том, в какой стране(-ах) будет осуществляться работа с Информацией.

Заказчик

Заместитель генерального директора
по техническим вопросам и
информационным технологиям
ПАО «Самараэнерго»

Исполнитель

Р.Л. Шуман
м. п.

м. п.

ЖУРНАЛ

инструктажа по

информационной безопасности

критической информационной инфраструктуры

ПАО «Самараэнерго»

Самара 2026

[illegible]