

РЕГЛАМЕНТ ВЗАИМОДЕЙСТВИЯ СТОРОН по обеспечению информационной безопасности

Общество с ограниченной ответственностью «Ново-Салаватская ПГУ» (государственный регистрационный № 1100266000812 от 10.08.2010) в лице _____, действующего на основании _____, именуемое в дальнейшем Сторона 1, с одной стороны, и _____ (государственный регистрационный № _____ от _____) в лице _____, действующего на основании _____, именуемое в дальнейшем Сторона 2, с другой стороны, именуемые в дальнейшем Стороны, пришли к соглашению о нижеследующем:

1. Сторона 2 обязуется:

1.1 Определить лиц, ответственных за обеспечение информационной безопасности (далее – ИБ) у Стороны 2, и не позднее 5 (пяти) рабочих дней с даты подписания настоящего Регламента обеими сторонами предоставить Стороне 1 список указанных лиц, содержащий Ф.И.О. ответственных лиц, а также их контактную информацию и сведения о каналах связи для оперативного взаимодействия. Взаимодействие сторон в рамках данного Регламента осуществляется через ответственных лиц за обеспечение информационной безопасности Стороны 2 и куратора, ответственного за реагирование на инциденты ИБ Стороны 1.

1.2 Предоставить Стороне 1 для согласования список работников (далее – Список) Стороны 2, которым планируется предоставление доступа к информационной инфраструктуре (далее – ИИ) Стороны 1. В список допускаются только граждане РФ. В случае изменения состава указанных работников, необходимо предоставить актуальный Список не позднее, чем за 5 (пять) рабочих дней до дня, с которого запрашивается предоставление доступа и/или предполагается ограничение доступа.

1.3 Реализовать антивирусную защиту на АРМ и серверах Стороны 2, обеспечив поддержку в актуальном состоянии лицензии и базы данных сигнатур.

1.4 Настроить автоматическую блокировку сеанса при бездействии до 10 (десять) минут на АРМ Стороны 2.

1.5 Ограничить на АРМ Стороны 2 доступ пользователей к настройкам систем инициализации (BIOS/UEFI).

1.6 Включить регистрацию событий безопасности (срок хранения журналов событий безопасности – не менее 180 календарных дней).

1.7 Реализовать двухфакторную аутентификацию пользователей на АРМ Стороны 2, с которых осуществляется удаленный доступ к ИИ Стороны 1.

1.8 Использовать для доступа к ИИ Стороны 1 средства вычислительной техники, которые не используются в личных целях и на которых выполняются корпоративные меры по обеспечению информационной безопасности Стороны 2.

1.9 Реализовать в отношении учетных записей Стороны 2 принцип наименьших привилегий.

1.10 Реализовать парольную политику с соблюдением следующих требований:

- установить длину паролей учетных записей не менее 10 символов, пароль должен содержать символы, относящиеся к трем из следующих четырех категорий: заглавные буквы, строчные буквы, цифры, специальные символы; установить сроки замены парольных фраз не более 90 дней для учетных записей пользователей и не более 30 дней для учетных записей привилегированных пользователей;

- установить запрет на повторное использование старых паролей (password reuse);

- не допускать хранения парольных фраз и/или иных аутентификационных данных, используемых работниками Стороны 2, в свободном доступе или в открытом виде, а также исключить их передачу третьим лицам;

- все парольные фразы должны соответствовать установленному у Стороны 2 уровню стойкости к атакам типа перебор методом грубой силы (bruteforce);

- пароли Стороны 2 не должны содержать персонифицированную информацию (имена, адреса, даты рождения, телефоны), устойчивые выражения;

- парольные фразы, используемые работниками Стороны 2 для аутентификации в инфраструктуре Стороны 1, не должны использоваться ими в инфраструктуре Стороны 2, а также в личных целях.

1.11 Сегментировать сети Стороны 2 и исключить доступность локальных ресурсов из сегмента демилитаризированной зоны.

1.12 Перед инсталляцией или обновлением исходных кодов библиотек или компонентов, разработанных сторонними разработчиками, проводить самостоятельно или совместно с разработчиком их инспектирование на предмет наличия уязвимостей, недеklarированных возможностей программного обеспечения.

1.13 Использовать методы безопасной разработки программного обеспечения, в том числе, проводить анализ программного кода, выявлять ошибки, уязвимости и недеklarированные возможности программного обеспечения.

1.14 Не допускать установку обновления программного обеспечения в основную инфраструктуру Стороны 1 / Стороны 2 до успешного завершения тестирования соответствующего обновления в тестовой (резервной) среде.

1.15 При тестировании массивов данных Стороны 1 использовать только синтетические (сгенерированные) материалы, не содержащие коммерческую тайну и иную конфиденциальную информацию, в том числе персональные данные.

1.16 В случае обнаружения любой активности, имеющей признаки

вредоносной, либо выявления инцидентов информационной безопасности при работе в ИИ Стороны 1 или в инфраструктуре Стороны 2:

- в течение 30 минут с момента обнаружения соответствующих обстоятельств направить уведомление об этом на электронную почту `ib@nspgu.ru` или сообщить об этом Стороне 1 любым иным доступным способом;

- незамедлительно выполнить все необходимые и доступные Стороне 2 мероприятия по реагированию и меры по ликвидации последствий вредоносной активности/инцидента информационной безопасности, а также по недопущению компрометации конфиденциальных материалов и аутентификационных данных Стороны 1, предоставив Стороне 1 письменный отчет о проведенных мероприятиях не позднее 48 часов после завершения таких мероприятий.

1.17 Организовать процесс резервного копирования критичных сервисов Стороны 2. Хранение резервных копий должно осуществляться в изолированном сегменте сети.

1.18 Обеспечить защиту почтовых сервисов Стороны 2 от фишинга.

1.19 Обеспечить выполнение процесса управления уязвимостями в инфраструктуре Стороны 2.

1.20 Обеспечить защищенное удаленное подключение с использованием средств криптографической защиты информации.

1.21 Обеспечить защищенный обмен файлами и информацией через файловое хранилище.

1.22 Организовать реализацию записи всех действий пользователей, включенных в Список, при осуществлении удаленного подключения к ИИ Стороны 1. Рекомендуемый срок хранения журналов событий не менее 1 года. В случае возникновения инцидента предоставлять указанные журналы событий Стороне 1.

1.23 Исключить подключение любых носителей данных к вычислительной технике Стороны 1. Информационный обмен осуществлять только через согласованные Стороной 1 способы обмена.

1.24 Исключить передачу информации, относящейся к производственной деятельности¹ посредством программ для обмена мгновенными сообщениями, программ аудио/видеоконференций, не входящих в состав Единого реестра российских программ для электронных вычислительных машин и баз данных², по открытым каналам телефонной, телеграфной и факсимильной связи, а также с использованием сети Интернет без принятия соответствующих мер защиты, удовлетворяющих обе стороны.

1.25 Исключить локальное использование в ИИ Стороны 1, а также на АРМ Стороны 2, используемом для подключения к ИИ Стороны 1, программного обеспечения для удаленного управления и администрирования, кроме

¹ Предусмотрено абзацем 10 ст. 209 Трудового кодекса Российской Федерации от 30.12.2001 N 197-ФЗ.

² Постановление Правительства РФ от 16 ноября 2015 г. N 1236 "Об утверждении Правил формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации".

согласованного со Стороной 1.

1.26 Исключить удаление, изменение приложений или блокирование их работы, а также работы сетевых сервисов на средствах вычислительной техники Стороны 1.

1.27 Исключить любое вмешательство в работу средств защиты информации Стороны 1, а также попытки обойти каким-либо способом их работу.

Не приносить, не скачивать, не запускать и/или не устанавливать любое несогласованное программное обеспечение, в том числе портативное (portable) программное обеспечение, а также прочую информацию, в том числе мультимедийные файлы и прочий контент на средствах вычислительной техники Стороны 1.

1.28 Обеспечить проведение работ в ИИ Стороны 1 только в рабочие³ дни с 9-00 до 17-00 (UTC+05:00, Екатеринбург), если иное не предусмотрено договором.

1.29 Осуществлять учет всех изменений ИИ Стороны 1 путем обязательного документирования выполненных работ. Учетные документы оформить в письменной форме и/или в электронном виде.

1.30 Производить обмен информацией; составляющей коммерческую тайну, или иной конфиденциальной информацией, только после заключения между сторонами Соглашения о конфиденциальности для юридических лиц и Договора о конфиденциальности для физических лиц, в соответствии с их условиями.

1.31 Обеспечить защиту информации ограниченного доступа, передаваемую по любым каналам связи, в том числе третьим лицам, в соответствии с действующими требованиями законодательства.

1.32 Сохранять конфиденциальность обрабатываемых персональных данных, использовать меры для их защиты от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных.

1.33 Не передавать документы, содержащие персональные данные, за исключением документов, содержащие персональные данные, полученные из общедоступных источников персональных данных:

- по открытым каналам связи, вычислительным сетям вне пределов контролируемой зоны, в том числе по электронной почте с использованием сети Интернет без применения мер по обеспечению безопасности персональных данных
- с применением средств факсимильной связи;
- иным незащищенным способом.

1.34 Не использовать документы (информацию), а также их копии, содержащие персональные данные субъектов персональных данных, в личных и

³ Согласно производственному календарю по Республике Башкортостан, утвержденному на период, соответствующему году проведения работ

иных целях, не связанных с исполнением обязанностей, для исполнения которых соответствующие документы (информация) были предоставлены.

1.35 Не фотографировать и не производить видеофиксацию информации, содержащую персональные данные, отображаемые на экранах мониторов АРМ.

1.36 Не хранить персональные данные на АРМ.

1.37 Исключить передачу (отправку) документов или информации, содержащих персональные данные любых субъектов персональных данных, на личные адреса электронной почты работников, в том числе, включенных в Список и/или личные адреса электронной почты третьих лиц.

1.38 В случае привлечения Стороной 2 субподрядной организации для работы в ИИ Стороны 1 или Стороны 2, обеспечить соблюдение представителями субподрядной организации требований, предусмотренных настоящим Регламентом.

2. Сторона 1 имеет право:

2.1 Отказать в предоставлении доступа к ИИ Стороны 1 любому представителю Стороны 2 и/или привлеченному специалисту субподрядной организации, включенному в Список лиц, допущенных к работе в ИИ.

2.2 Полностью или частично приостановить любому представителю Стороны 2 и/или привлеченному специалисту субподрядной организации, включенному в Список лиц, допущенных к работе в ИИ, доступ к ИИ Стороны 1.

2.3 Требовать исключения лица, нарушившего требования настоящего Регламента, из согласованного Списка лиц, допущенных к работе в ИИ Стороны 1;

2.4 Фиксировать факты нарушений Регламента Стороной 2.

2.5 В случае нарушения Регламента Стороной 2 требовать выплаты штрафа в размере, установленном в Классификаторе нарушений требований информационной безопасности (Приложение 1), а также компенсации в полном размере убытков, возникших в связи с нарушением. Убытки взыскиваются сверх суммы штрафа.

2.6 Запрашивать у Стороны 2 политики информационной безопасности, результаты внутренних и/или внешних аудитов информационной безопасности, результаты тестирования на проникновение инфраструктуры, план реагирования на компьютерные инциденты, а также регламент действия работников в случае нештатных ситуаций и иные документы, связанные с обеспечением ИБ.

2.7 Проводить оценку соблюдения требований по обеспечению информационной безопасности любыми доступными способами, не противоречащими нормам законодательства РФ. Для этого Сторона 1 направляет письменное уведомление о проведении оценки не менее чем за 10 (десять) рабочих дней до ее начала. При получении указанного уведомления Сторона 2 обязана обеспечить возможность проведения оценки соблюдения требований по обеспечению информационной безопасности, а также оказать Стороне 1 содействие в проведении такой оценки в объеме, определенном уведомлением Стороны 1, а также дополнительными обращениями, направленными Стороне 2 в процессе проведения оценки.

3. Оформление нарушений

3.1 Факт нарушения требований по обеспечению информационной безопасности фиксируется по форме «Акт о выявленном нарушении» (Приложение 2).

3.2 В случае обнаружения нарушений, связанных с обеспечением информационной безопасности в ИИ, Сторона 1 направляет Стороне 2 уведомление, в котором приводится описание нарушений.

3.3 Не позднее 5 (пяти) рабочих дней с даты получения уведомления о нарушении, Сторона 2 обязана рассмотреть такое уведомление, направить Стороне 1 ответ с указанием предполагаемых причин возникновения нарушения и направить представителям Стороны 2 для расследования причин и согласования со Стороной 1 мер, порядка и сроков исправления, а также подписания Акта о выявленном нарушении. Если в указанный срок Сторона 2 не направила ответ с указанием предполагаемых причин возникновения нарушения и не направила представителя Стороны 2 для расследования причин выявленного нарушения и согласования со Стороной 1 мер, порядка и сроков исправления, а также подписания Акта о выявленном нарушении, считается, что Сторона 2 согласна с причинами возникновения инцидента, изложенными в уведомлении Стороны 1 об обнаружении нарушения, при этом Акт о выявленном нарушении, подписанный Стороной 1 в одностороннем порядке, имеет силу двустороннего. В случае если представитель Стороны 2 отказывается от подписания акта о выявленном нарушении, для выяснения причин выявленного нарушения Сторона 1 привлекает независимую экспертную организацию. Расходы, связанные с таким привлечением экспертной организации, несет Сторона 2, за исключением случаев, если, согласно выводам, заключения экспертной организации, выявленные Стороной 1 нарушения не будут подтверждены.

Сторона 1

Сторона 2

_____ / _____

_____ / _____

Классификатор нарушений требований
информационной безопасности работниками Стороны 2

№	Вид нарушения	Размер штрафа (тыс. руб.)	
		Однократное нарушение	Повторное нарушение
1	Нарушение требований информационной безопасности	100	150
2	Нарушение условий обмена информацией, составляющей коммерческую тайну, и иную конфиденциальную информацию, предусмотренных Соглашением о конфиденциальности ⁴	100	150

Сторона 1

_____ / _____

Сторона 2

_____ / _____

⁴ В случае, если в результате нарушения условий обмена произошла утечка конфиденциальных данных, также взыскиваются убытки в соответствии с требованиями законодательства РФ.

АКТ
о выявленном нарушении № __________
(дата, время, место составления акта)Мною _____
(фамилия, имя, отчество, должность)в присутствии _____
(фамилии, имена, отчества, должности лиц, присутствовавших при составлении акта)составлен акт о том, что представителем _____
(организация, фамилия, имя, отчество, должность)было допущено следующее нарушение: _____
(дата, время совершения нарушения,
описание нарушения, ссылка на соответствующий пункт регламента, соглашения о конфиденциальности, договора и т.п.)

Подпись лица, выявившего нарушение / составившего акт: _____ (_____)

Подписи лиц, присутствующих при составлении акта: _____ (_____)

_____ (_____)

Пояснения представителя Стороны 2 _____
(при несогласии указать причину несогласия)С актом ознакомлен, экземпляр акта получил _____
(подпись представителя Стороны 2, Ф.И.О., дата)Приложения: _____
(объяснительная, другие материалы)_____
(Ф.И.О. представителя Стороны 2, должность)был ознакомлен с актом _____
(дата и время ознакомления)

письменно подтвердить ознакомление с актом и получение экземпляра акта отказался.

Факт отказа от подписания (получения) акта подтверждаем:

Должность _____
(подпись, Ф.И.О., дата и время)Должность: _____
(подпись, Ф.И.О., дата и время)Должность: _____
(подпись, Ф.И.О., дата и время)

Сторона 1

Сторона 2