УТВЕРЖДЕНЫ

приказом ОАО «Севернефтегазпром»

от 22 . 06 .2022 № 436

ПРАВИЛА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ ПОЛЬЗОВАТЕЛЕЙ В КОРПОРАТИВНОЙ СЕТИ ОАО «СЕВЕРНЕФТЕГАЗПРОМ»

г. Новый Уренгой
2022 год

СОДЕРЖАНИЕ:

1. Общие положения

1.1. Назначение, область применения

1.1.1. Правила обеспечения информационной безопасности при работе пользователей в корпоративной сети ОАО «Севернефтегазпром» (далее – Правила) раскрывают положения Политики информационной безопасности ОАО «Севернефтегазпром» и разработаны в соответствии с требованиями законодательства Российской Федерации, рекомендаций ПАО «Газпром».

1.1.2. Настоящие Правила регламентируют работу пользователей единой корпоративной информационной системы ОАО «Севернефтегазпром» (далее – Общество) в процессе её эксплуатации, регулируют порядок получения допуска пользователей к работе с ЕКИС, устанавливают требования по обеспечению ИБ при работе с ЕКИС, ответственность за их невыполнение.

1.1.3. Положения настоящих Правил обязательны для исполнения всеми работниками Общества, получившими доступ к ЕКИС и являющимися пользователями ЕКИС.

1.1.4. Положения настоящих Правил обязательны для исполнения всеми представителями сторонних организаций, которым для исполнения договорных отношений необходимо предоставление доступа к ЕКИС.

1.2. Нормативные ссылки, термины, определения и сокращения

1.2.1. Нормативные ссылки:

Р Газпром 4.2-0-001-2009 «Типовая Политика информационной безопасности дочернего общества (организации)»;

СТО Газпром 4.2-1-001-2009 Система обеспечения информационной безопасности ПАО «Газпром». Основные термины и определения (далее – СТО Газпром 4.2-1-001-2009);

Политика информационной безопасности ОАО «Севернефтегазпром»;

Политика обеспечения информационной безопасности при взаимодействии со сторонними организациями ОАО «Севернефтегазпром»;

Политика управления инцидентами информационной безопасности ОАО «Севернефтегазпром».

1.2.2. В настоящих Правилах используются термины в соответствии с СТО Газпром 4.2-1-001-2009.

1.2.3. В настоящих Правилах используются следующие сокращения:

АРМ – автоматизированное рабочее место;

ИБ – информационная безопасность;
ПО – программное обеспечение;
СИУС – служба информационно-управляющих систем.
Pin-код – разновидность пароля на ключевом носителе или смарт-карте, для доступа к сервисам Общества или эксплуатации электронной подписи;
ЕКИС – единая корпоративная информационная система.

2. Порядок получения и блокирования доступа к работе с ЕКИС

2.1. Пользователем ЕКИС может являться работник структурного подразделения Общества либо представитель сторонней организации.

2.2. Для работы с ЕКИС за пользователем должен быть закреплен минимальный набор прав и ограничений, необходимый для беспрепятственного исполнения его должностных (трудовых) обязанностей либо договорных отношений.

2.3. Закрепление набора прав, ограничений и доступ работника Общества к работе с ЕКИС осуществляется в следующем порядке:

2.3.1. Руководители структурных подразделений Общества, при необходимости получения работниками доступа к ЕКИС, в контуре «Система заявок» системы электронного документооборота на основе типовой конфигурации «1С: Документооборот 8 КОРП», редакции 2.1 (далее – Система заявок), оформляют заявки на предоставление доступа к ЕКИС, подписывают их и при необходимости получения доступа (ограниченный доступ) к информационному ресурсу согласовывают данные подключения с обладателем информации. В заявках перечисляются права доступа пользователей, информационные ресурсы, на которые распространяются права, дни доступа и время работы работника структурного подразделения. После этого данные заявки передаются в отдел информационной безопасности на согласование.

2.3.2. Оформленные и согласованные с отделом информационной безопасности заявки обрабатываются СИУС, работники которой в течение трёх рабочих дней осуществляют подключение доступа работников Общества к работе с ЕКИС в объеме, соответствующем заявке. Доступ к ЕКИС осуществляется по уникальной учетной записи, присваиваемой каждому пользователю СИУС.

2.3.3. Устные указания о предоставлении доступа от любого работника Общества к работе с ЕКИС запрещены для исполнения СИУС.

2.4. Предоставление прав доступа представителям сторонних организаций к ЕКИС запрещается до заключения договора о

конфиденциальности между Обществом и сторонней организацией, и осуществляется в порядке, предусмотренном п. 2.3. настоящих Правил.

2.5. Блокировка доступа пользователей к ресурсам ЕКИС осуществляется администратором ИБ или работниками СИУС в следующих случаях:

пользователю более не требуется доступ к ресурсу ЕКИС Общества (увольнение работника, изменение должностных обязанностей, перевод в другое структурное подразделение, длительный перерыв в выполнении должностных (трудовых) обязанностей более четырёх месяцев, прекращение договорных отношений со сторонней организацией);

выявления признаков инцидентов ИБ, связанных с доступом пользователя к ресурсам ЕКИС Общества;

по результатам пересмотра прав доступа и привилегий пользователей.

2.6. В случае увольнения работника или длительного перерыва в выполнении должностных (трудовых) обязанностей более четырёх месяцев доступ к ресурсам ЕКИС блокируется автоматически с даты издания приказа об увольнении или даты начала длительного перерыва.

2.7. В случае отсутствия необходимости доступа к ЕКИС пользователю Общества (в результате пересмотра прав доступа и привилегий пользователей или поступившего запроса от владельца информационного ресурса), работник отдела информационной безопасности направляет уведомление в СИУС и руководителю структурного подразделения работника Общества о необходимости блокирования доступа пользователю ЕКИС с указанием причины блокировки. Уведомления направляются по средством корпоративной электронной почты или в Системе заявок. Факт направления уведомления работник отдела информационной безопасности вносит в электронный реестр уведомлений об инцидентах.

2.8. В случае выявления признаков инцидента ИБ, доступ временно (не более суток) блокируется работником СИУС, либо автоматически с обязательным согласованием блокирования с отделом информационной безопасности. Блокирование проводится в целях идентификации и анализа инцидента ИБ и минимизации воздействия на работоспособность ЕКИС Общества. По результатам анализа группой реагирования на инциденты ИБ принимается решение о возможности разблокирования доступа к информационным ресурсам пользователю ЕКИС.

Разблокирование доступа работником СИУС разрешено только по согласованию с отделом информационной безопасности.

2.9. Руководители структурных подразделений при увольнении, переводе в другое структурное подразделение работников Общества, имеющих допуск к работе с ЕКИС, обязаны письменно уведомить об этом

отдел информационной безопасности и СИУС за пять дней до наступления указанных событий.

3. Требования по обеспечению информационной безопасности

3.1. Руководители структурных подразделений Общества предоставляют работникам настоящие Правила для ознакомления (под роспись). Знание и исполнение настоящих Правил строго обязательно для всех пользователей ЕКИС.

3.2. Перед предоставлением доступа представителям сторонней организации к ЕКИС Общества необходимо расписаться в листе ознакомления с настоящими Правилами.

3.3. Пользователь ЕКИС обязан:

выполнять требования по защите информации при работе в ЕКИС;

применять АРМ и ЕКИС только для выполнения должностных (трудовых) обязанностей либо договорных отношений;

работать в ЕКИС только в разрешенный период времени;

при сообщениях тестовых программ (антивирусное ПО, антишпионское ПО и т.д.) о наличии «вирусов» немедленно докладывать в отдел информационной безопасности и СИУС;

для выполнения политики ИБ Общества при работе со сведениями, составляющими коммерческую тайну и иную конфиденциальную информацию Общества, использовать только зарегистрированные съемные носители информации;

в случае необходимости использования носителей информации, поступивших из других структурных подразделений Общества, учреждений, предприятий и организаций, до начала использования носителя проводить проверку данных носителей на отсутствие «вирусов» при помощи корпоративного антивирусного ПО;

передавать сведения, составляющие коммерческую тайну и иную конфиденциальную информацию Общества, используя средства криптографической защиты в соответствии с утвержденными в Обществе Инструкцией по конфиденциальному делопроизводству в ОАО «Севернефтегазпром» и Регламентом обеспечения ИБ при использовании средств криптографической защиты информации в ОАО «Севернефтегазпром»;

предоставлять АРМ, находящиеся в служебном пользовании:

работникам отдела информационной безопасности Общества для проверок состояния защиты информации и выявления возможных каналов утечки от несанкционированного доступа к защищаемой информации;

работникам СИУС Общества для выполнения текущего обслуживания, сервисных и профилактических работ, проведения инвентаризации аппаратного и программного обеспечения;

администраторам и аудиторам ИБ Общества для реализации и контроля выполнения мер по обеспечению ИБ.

3.4. Требования к пользователю ЕКИС по сохранности сведений об уникальной учетной записи (пароля и pin-кода).

Все пользователи ЕКИС обязаны:

хранить данные уникальных учетных записей в тайне от посторонних лиц;

не сообщать свой пароль (pin-код) другому лицу, даже если это вышестоящее должностное лицо;

вводить учетные данные, убедившись, что средства ввода (клавиатура, экранная клавиатура и т.д.) находятся вне поля зрения других лиц;

периодически производить смену пароля (pin-кода), не реже 1 раза в 30 дней для административных и пользовательских учетных записей.

соблюдать следующие требования, предъявляемые к использованию пароля (pin-кода):

длина пароля (pin-кода) пользовательских учетных записей должена состоять не менее чем из 10 (десяти) символов, с использованием верхних и нижних регистров, цифр и специальных символов (@, #, $, &, *, % и т.п.);

длина пароля (pin-кода) административных учетных записей должена состоять не менее чем из 16 (шестнадцати) символов, с использованием верхних и нижних регистров, цифр и специальных символов (@, #, $, &, *, % и т.п.);

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

при смене пароля (pin-кода) новое значение должно отличаться от предыдущего не менее чем в четырех позициях;

незамедлительно сообщать в отдел информационной безопасности и СИУС Общества о подозрениях в несанкционированном доступе посторонних лиц к АРМ или компрометации паролей (pin-кодов) и следовать дальнейшим предписаниям для предотвращения ущерба для Общества.

3.5. Пользователю ЕКИС запрещается:

3.5.1. Фиксировать свои уникальные учетные данные (пароли, pin-коды, идентификаторы и др.) на твердых носителях (в т.ч. на бумаге).

3.5.2. Самовольно вносить изменения в конструкцию и конфигурацию АРМ, а также изменять настройки других узлов ЕКИС.

3.5.3. Самовольно перемещать АРМ, а также другие узлы ЕКИС.

В случае производственной необходимости перемещения АРМ уведомлять об этом любым корпоративным доступным средством начальника СИУС.

3.5.4. Самовольно нарушать пломбы, которыми опечатаны системные блоки, в случае обнаружения срыва пломбы, пользователь ЕКИС обязан сообщить об этом в отдел информационной безопасности и СИУС.

3.5.5. Самостоятельно производить установку любого ПО.

3.5.6. Сохранять на своих АРМ дистрибутивы системных или прикладных программ, не входящие в состав ПО, утвержденного для установки на АРМ.

3.5.7. Оставлять свой АРМ без блокировки с функцией защиты паролем (pin-кодом).

3.5.8. Допускать к АРМ посторонних лиц.

3.5.9. Использовать для авторизации в ЕКИС не принадлежащие пользователю учетные данные.

3.5.10. Запускать на АРМ Общества любые системные или прикладные программы, не входящие в состав ПО, утвержденного для использования на АРМ.

3.5.11. Производить копирование сведений, составляющих коммерческую тайну, и иную конфиденциальную информацию Общества, на неучтенные носители информации (в том числе и для временного хранения информации).

3.5.12. Хранить на АРМ информацию, которая не относится к выполнению должностных (служебных) обязанностей, в том числе графические, аудио- и видеоматериалы.

3.5.13. Передавать сведения, содержащие коммерческую тайну и иную конфиденциальную информацию Общества, по открытым каналам связи, без использования средств шифрования.

3.5.14. Работать на АРМ с защищаемой информацией Общества при обнаружении неисправностей.

4. Правила работы с ресурсами сети Интернет

4.1. Допуск пользователей к сети Интернет осуществляется в соответствии с разделом 2 настоящих Правил в соответствии с полномочиями, указанными в заявке.

4.2. При работе с ресурсами сети Интернет пользователям запрещается:

использовать рабочее время и ресурсы сети Интернет в личных целях;

разглашать информацию Общества, включенную в Перечень информации, составляющей коммерческую тайну, и иную

конфиденциальную информацию Общества, ставшую известной пользователю Общества в процессе исполнения им своих служебных (трудовых) обязанностей либо договорных отношений, либо иным путем;

распространять защищаемые авторскими правами материалы, затрагивающие какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

загружать, распространять материалы, содержащие вирусы или другие вредоносные компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, учетные данные (имена пользователей, пароли, pin-коды) и прочие средства для получения несанкционированного доступа к платным ресурсам в сети Интернет, а также размещать ссылки на вышеуказанную информацию;

посещать ресурсы, создавать, распространять информационные материалы и сообщения, содержащие оскорбительную или провокационную информацию;

несанкционированно распространять информацию рекламного характера;

использовать для приема и передачи информации публичные сервисы сети Интернет любого характера и назначения (например, disk.yandex.ru, files.mail.ru и т.д.);

применять программные средства удаленного управления АРМ и использовать таковые в любом виде;

использовать адрес корпоративной электронной почты для регистрации в публичных сервисах, если персонализированный доступ к публичному сервису (или получение информации от публичных сервисов) не требуется для выполнения служебных (договорных) обязанностей;

самостоятельно изменять конфигурацию ПО, используемого для доступа в сеть Интернет;

использовать специальные программные средства обеспечения анонимности доступа в сеть Интернет;

подтверждать любые запросы ресурсов в сети Интернет на установку любого ПО, а также на переход на другие ресурсы сети Интернет, если они не известны пользователю.

4.3. Отдел информационной безопасности и СИУС периодически на выборочной основе проверяют статистику посещения ресурсов сети Интернет. В случае выявления факта использования ресурсов сети Интернет

в непроизводственных целях или содержание и направленность которых запрещены законодательством Российской Федерации, проводится отключение пользователя от сети Интернет в следующем порядке:

при выявлении факта посещения ресурсов сети Интернет пользователем не в служебных целях в соотношении более 50 % скачанного трафика или по количеству посещаемых страниц за один день, нарушителю посредством электронной почты предоставляется отчет и предлагается в течение двух рабочих дней предоставить обоснование;

в случае непредоставления обоснования или недостаточного обоснования нарушения использования ресурсов Интернета, отдел информационной безопасности совместно с СИУС принимает коллегиальное решение об отключении нарушителя от доступа в сеть Интернет. СИУС проводит отключение от сети Интернет пользователя с последующим уведомлением по электронной почте.

В дальнейшем повторное подключение доступа в сеть Интернет производится СИУС на основании служебной записки (обоснования) на имя владельца информационного ресурса с положительной резолюцией начальника отдела информационной безопасности.

4.4. Вся информация о ресурсах, посещаемых пользователями, протоколируется на веб-серверах СИУС и проверяется отделом информационной безопасности.

5. Правила работы с корпоративной электронной почтой

5.1. Электронная почта является собственностью Общества и может быть использована исключительно в служебных целях. Использование электронной почты в личных целях категорически запрещено.

5.2. Содержимое электронного почтового ящика работника Общества может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

5.3. Пересылка/отправка материалов за пределы Общества (сторонним пользователям) осуществляется в соответствии с требованиями законодательства Российской Федерации, Политиками ИБ Общества и Правилами.

5.4. Пересылка/отправка материалов объемом свыше 5 Мбайт необходимо осуществлять через облачное хранилище Общества. Исключением является:

5.4.1 Отправка материалов уполномоченным лицам акционеров Общества, членам Совета директоров, Ревизионной комиссии, Комитета по техническим вопросам Совета директоров (напрямую, а также их

уполномоченным лицам) в рамках подготовки и проведения корпоративных событий, осуществляемая в установленном внутренними документами Общества порядке отделом корпоративного регулирования с электронного адреса: okr@sngp.com. В указанных случая объем отправки может быть в пределах 15 Мбайт. По согласованию с отделом ИБ объем отправки может быть увеличен до 20 Мбайт.

5.4.2. Пересылка/отправка материалов муниципальным, государственным, контролирующим, надзорным, правоохранительным и судебным органам объемом свыше 5 Мбайт при согласовании с отделом ИБ.

5.5. При работе с корпоративной системой электронной почты работникам Общества запрещается:

использовать адрес корпоративной почты для оформления подписок, без предварительного согласования с отделом информационной безопасности и СИУС Общества;

публиковать свой адрес, либо адреса других работников Общества на общедоступных Интернет ресурсах (форумы, конференции и т.п.);

открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма был ранее известен;

осуществлять массовую рассылку почтовых сообщений внешним и внутренним адресатам без их на то согласия, кроме уполномоченных работников Общества. Данные действия квалифицируются как рассылка СПАМ и являются незаконными;

осуществлять массовую рассылку почтовых сообщений уполномоченными работниками в пределах Общества объёмом свыше 5 Мбайт. Материалы объёмом свыше 5 Мбайт, предназначенные для ознакомления работников Общества, необходимо располагать на сетевом ресурсе общего пользования, и сетевые ссылки на размещённые материалы указывать в электронном сообщении;

пересылать/отправлять материалы объёмом свыше 5 Мбайт за пределы Общества (сторонним пользователям). Передача файлов объёмом более 5 Мбайт осуществляется через корпоративное облачное хранилище за исключением случаев, указанных в п. 5.4.1. и п. 5.4.2. настоящих Правил;

осуществлять массовую рассылку почтовых сообщений рекламного характера без предварительного согласования с отделом информационной безопасности;

пересылать/отправлять через электронную почту материалы, содержащие вирусы или другие вредоносные компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или

телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли, pin-коды и прочие средства для получения несанкционированного доступа к платным ресурсам в сети Интернет, а также ссылки на вышеуказанную информацию;

распространять защищаемые авторскими правами материалы, затрагивающие какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

распространять информацию содержание и направленность, которой запрещены законодательством Российской Федерации, включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.;

передавать сведения, содержащие коммерческую тайну и иную конфиденциальную информацию Общества, без использования средств криптографической защиты информации;

предоставлять посторонним лицам учетные данные для доступа к своему почтовому ящику.

6. Ответственность за несоблюдение требований настоящих Правил

6.1. Ответственность работников Общества за несоблюдение требований настоящих Правил, повлекших за собой разглашение или утрату информации ограниченного доступа, определяется законодательством Российской Федерации, внутренними нормативными документами Общества, а также должностными инструкциями работников Общества.

6.2. Ответственность сторонних организаций за несоблюдение требований настоящих Правил, повлекших за собой разглашение или утрату информации ограниченного доступа, определяется законодательством Российской Федерации, договорными отношениями между сторонними организациями и Обществом.

7. Контроль за соблюдением требований настоящих Правил

Контроль за соблюдением требований настоящих Правил осуществляет отдел информационной безопасности.

8. Порядок пересмотра

8.1. Настоящие Правила должны пересматриваться отделом информационной безопасности Общества с периодичностью не реже одного раза в два года. При пересмотре настоящих Правил должны учитываться результаты контроля эффективности обеспечения ИБ за предыдущий период.

8.2. Процедура пересмотра настоящих Правил должна включать следующие мероприятия:

анализ и выявление несоответствий действующих Правил текущим условиям;

разработку предложений по совершенствованию Правил;

утверждение новой редакции Правил генеральным директором Общества.

8.3. При осуществлении процедуры пересмотра должны учитываться:

результаты контроля состояния ИБ и предложения структурных подразделений о совершенствовании процедур обеспечения ИБ;

изменения в организационно-штатной структуре Общества и в его информационной инфраструктуре;

изменения в нормативно-правовой базе в области ИБ, произошедшие с момента утверждения предыдущих Правил;

результаты анализа произошедших инцидентов ИБ, а также уязвимости и угрозы, выявленные в Обществе за время, прошедшее с момента утверждения предыдущих Правил;

изменения в управлении ИБ, включая изменения в распределении ресурсов и обязанностей при обеспечении ИБ.

Приложение № 2
к приказу ОАО «Севернефтегазпром»
от 22.06.2022 № 436

Лист ознакомления с приказом «____» _____ 20 __ г.1

Правила обеспечения информационной безопасности при работе пользователей в корпоративной сети ОАО «Севернефтегазпром»

Наименование СП _____

№ п/п	Должность работника СП	ФИО работника СП	Дата ознакомления	Подпись
1.				
2.				
3.				
…				

[1] Оригинал листа ознакомления с ЛНА хранится в структурном подразделении Общества, сканированная копия направляется в отдел информационной безопасности СКЗ