# Приложение 9.2

# К Договору №\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_от «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г

# Требования

# информационной безопасности (далее – «Требования»)

**Термины, определения и сокращения:**

**ПО –** Программное обеспечение;

**Экономическая безопасность (ЭБ)** – подразделение Предприятия, в зоне ответственности которого находится информационная безопасность и техническая защита;

**Пользователь** – работник Контрагента, работник третьего лица, привлеченного Контрагентом с письменного согласия Предприятия;

**Корпоративная сеть -** объединение информационных систем, компьютерного, телекоммуникационного и офисного оборудования всех функций и направлений деятельности Предприятия, посредством их подключения к единой компьютерной сети передачи данных с использованием различных физических и логических каналов связи, отделенных от публичных сетей передачи данных.

Контрагент обязан до предоставления конкретным Пользователям доступа к Корпоративной сети ознакомить всех Пользователей, которым планируется предоставить такой доступ, с настоящими Требованиями.

Контрагент обязан в случае привлечения с письменного согласия Предприятия третьих лиц включить в заключаемые с ними договоры условия, предусмотренные настоящими Требованиями, и осуществлять контроль их исполнения. По требованию Предприятия Контрагент обязан предоставить копии договоров, заключенных им с третьими лицами и, в случае наличия у Предприятия замечаний по их тексту, обеспечить внесение в договоры соответствующих изменений.

# Требования по соблюдению информационной безопасности в Корпоративной сети

* 1. Контрагент обязан перед началом использования Корпоративной сети Предприятия обеспечить ознакомление Пользователей с требованиями локальных актов Предприятия, в том числе по обеспечению информационной безопасности.

1.2 Пользователям запрещается:

* передавать другим лицам или разглашать в любой форме:
  + персональные атрибуты доступа в корпоративную сеть и к информационным активам;
  + собственные права доступа и полномочия в информационных системах без получения согласования непосредственного руководителя и ЭБ Предприятия.
* использовать уязвимости или дефекты в защите информационных систем для нанесения ущерба этим системам, для расширения персональных полномочий, для осуществления несанкционированного доступа к хранящейся в них информации. Так же запрещается использование ПО, не имеющего отношения к выполнению функций и задач, в связи с которыми предоставлен доступ к Корпоративной сети;
* подключать к MS AD оборудование, не принадлежащее Предприятию;
* осуществлять поиск уязвимостей информационных систем Предприятия;
* преднамеренно записывать, создавать, компилировать, копировать, распространять, запускать на выполнение или пытаться встраивать любые машинные коды, разработанные для самовоспроизводства, повреждение или создание любых других помех функционированию информационных систем Предприятия и нормальной работе других пользователей;
* использовать ресурсы Корпоративной сети Предприятия для получения несанкционированного доступа к любым компьютерным сетям (информационным системам) или каким-либо образом создавать помехи, изменять, нарушать их функционирование, а также размещать информацию, запрещенную к распространению в соответствии с действующим законодательством РФ;
* неправомерный доступ к охраняемой законом компьютерной информации, если это деяние может повлечь уничтожение, блокирование, модификацию либо копирование компьютерной информации;
* устанавливать, использовать любые программные или аппаратные средства, позволяющие обезличивать, скрывать их действия в Корпоративной сети;
* устанавливать, использовать средства удаленного доступа или управления, использующие сервера в публичных сетях передачи данных;
* предпринимать действия для получения актуальных действующих паролей, наименований учетных записей и любых других данных, которые могут быть использованы для получения несанкционированного доступа к информационным ресурсам Корпоративной сети Предприятия. Исключением является информирование уполномоченных работников Предприятия, которым могут потребоваться сведения об учетной записи и полномочиях Пользователей;
* предоставлять доступ через корпоративную сеть к локальным ресурсам своего оборудования другим Пользователям;
* использовать для обработки конфиденциальной информации Предприятия не принадлежащее Предприятию оборудование и программное обеспечение.
  1. Письменно извещать Предприятие не менее чем за 5 (пять) рабочих дней до даты увольнения Пользователей или их отстранения от осуществления действий, связанных с использованием

# Основные требования по применению паролей

* 1. Пароли являются основным механизмом аутентификации пользователя в информационных системах Предприятия. Несоблюдение правил выбора, хранения и использования паролей может привести к нарушению конфиденциальности, целостности либо доступности информации, обрабатываемой в информационных системах Предприятия и повлечь причинение имущественного и других видов ущерба интересам Предприятия.
  2. Для осуществления первичного входа в информационную систему пользователю предоставляется временный пароль доступа. При получении временного пароля пользователь обязан произвести смену этого пароля. В дальнейшем пользователь должен осуществлять смену своих паролей самостоятельно не реже чем 1 раз в 30 дней.
  3. С целью предотвращения несанкционированного доступа к рабочим местам Пользователей, а также к ресурсам Корпоративной сети с использованием чужих учетных записей (имен Пользователей), Пользователи обязаны блокировать доступ к своему оборудованию в случае оставления ими своего рабочего места нажатием на компьютерной клавиатуре набора клавиш Ctrl+Alt+Del и далее - кнопки «Блокировка» (для Microsoft Windows XP), или «Блокировать компьютер» (для Microsoft Windows 7), или используя сочетание клавиш Win+L, или другим предусмотренным для используемой операционной системы способом.
  4. Все выбираемые Пользователями пароли должны отвечать приведенным ниже требованиям:
* содержать не менее 8 символов;
* содержать 3 любых вида символов из 4: строчные буквы, заглавные буквы, цифры, спецсимволы;
* не повторять ни один из 24 предыдущих паролей;
* не являться словом из словаря, сленга, диалекта, жаргона;
* не являться личной информацией (например, для создания паролей не должны применяться имена членов семьи, адреса, телефоны, даты рождения);
* не состоять из последовательностей символов раскладок клавиатуры (к примеру, 123456qwerty, 1qaz2wsx).
* Рекомендуется выбрать пароли, в которых будет выполнено хотя бы одно из следующих условий:
* несколько слов написаны слитно;
* при наборе слова на клавиатуре использованы клавиши, смещенные относительно нужных на один ряд вверх, вниз, вправо или влево;
* слово набрано со смещением на определенное количество букв вверх или вниз по алфавиту;
* произвольная комбинация цифр и обычного слова;
* намеренно неправильное написание слова (но не обычная в данном слове орфографическая ошибка).
  1. Пользователи обязаны соблюдать необходимые меры предосторожности для обеспечения конфиденциальности своих паролей.
  2. Запрещается:
* сообщать или разглашать свой пароль кому-либо, включая коллег, руководителей и работников службы технической поддержки, любыми средствами и способами;
* записывать, хранить пароли учетных записей Пользователей в доступной для чтения форме в любом виде;
* использовать автоматическое сохранение пароля при входе в информационные системы любого характера и назначения;
* использовать одинаковые пароли в различных информационных системах;
* использовать общие пароли в информационных системах, принадлежащих Предприятию, совместно с другими работниками.
  1. Пароль должен быть немедленно изменен, если имеются основания полагать, что данный пароль стал известен кому-либо еще, кроме самого Пользователя.
  2. Все текущие операции с паролем Пользователи должны осуществлять лично, не допуская возможности рассмотреть состав вводимого пароля и порядок введения символов.
  3. Формы ввода пароля в информационные системы должны скрывать вводимые символы.
  4. Пользователям запрещается предпринимать какие-либо действия по получению (раскрытию) паролей, не принадлежащих им учетных записей.

# Основные требования по антивирусной безопасности

* 1. На всех автоматизированных рабочих местах, подключаемых к информационным системам Предприятия, должно быть установлено лицензионное и сертифицированное для применения антивирусное ПО.
  2. Пользователям запрещается:
* несогласованная ЭБ Предприятия деинсталляция или деактивация антивирусного ПО, а также изменение его настроек;
* создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.
  1. Перечень правил по минимизации рисков заражения вредоносным ПО:

Во избежание заражения Корпоративной сети Предприятия вредоносным ПО Контрагент обязан обеспечить соблюдение всеми Пользователями следующих правил:

* + 1. В случае сомнений в наличии или в корректной работе на компьютере антивирусного ПО необходимо незамедлительно сообщить об этом Предприятию.
    2. Запрещается открывать какие-либо файлы, находящиеся во вложениях к электронным письмам, которые отправлены с подозрительных или неизвестных Пользователям адресов, пересылать их другим адресатам. В случае получения таких писем следует немедленно их удалить из папки «Входящие», а затем удалить их из папки «Удаленные» для того, чтобы исключить возможность их восстановления.
    3. В случае возникновения подозрений на наличие зараженных файлов во вложениях к сообщениям электронной почты (например, подозрительные имена или расширения файлов вложений, подозрительный источник сообщения, неизвестный отправитель с адресом электронной почты публичного почтового сервиса), которые однако могут быть полезны Пользователям для целей выполнения ими их функций, в связи с которыми был предоставлен доступ к Корпоративной сети, необходимо незамедлительно сообщить об этом Предприятию для проведения проверки подозрительного сообщения.
    4. Запрещается загружать файлы и соглашаться на предложения загрузить или установить ПО с неизвестных Пользователям Интернет сайтов. В случае возникновения сомнений в благонадежности сайта, но при необходимости дальнейшей с ним работы, необходимо обратиться к Предприятию для проведения проверки.
    5. Запрещается использовать на рабочих местах съемные носители информации без служебной необходимости, особенно если эти носители получены из неизвестных или подозрительных источников или могли использоваться на других компьютерах, возможно, незащищенных антивирусными программами. В случае служебной необходимости следует обратиться к Предприятию для проведения соответствующей проверки. Допускается самостоятельно осуществлять антивирусные проверки при помощи штатного антивирусного ПО, установленного на рабочих местах Пользователей.
    6. Запрещается допускать к рабочим местам других лиц. Для совместной работы или хранения важной, конфиденциальной информации необходимо использовать сетевые ресурсы на файловом хранилище, специально для этого предназначенные. В случае появления сообщений антивирусного ПО об обнаружении угрозы необходимо убедиться, что угроза успешно предотвращена. В ином случае, необходимо незамедлительно обратиться к Предприятию для принятия необходимых мер.
    7. В случае обнаружения признаков заражения компьютера вредоносным ПО (включая значительное увеличение времени отклика компьютера на действия Пользователей в любых программах, появление сообщения об ошибках, необъяснимая потеря файлов, изменение дат обновления файлов, увеличение размера файлов, системные сбои (включая случаи, когда операционная система перестает загружаться), а также любые другие необычные явления в работе компьютера, необходимо незамедлительно сообщить об этом Предприятию. Это позволит минимизировать ущерб, наносимый компьютерным вирусом, и принять необходимые меры для предотвращения повторного заражения.

# Основные требования по использованию ресурсов сети Интернет

* 1. На основании действующего законодательства РФ Предприятие может передать информацию о действиях Пользователей в сети Интернет уполномоченным на это третьим лицам, в том числе в правоохранительные органы. Использование права доступа в Интернет означает согласие Пользователей с тем, что за их деятельностью осуществляется контроль.
  2. При работе в сети Интернет Пользователям запрещается:

посещение ресурсов, создание и распространение информационных материалов и сообщений, содержащих оскорбительную или провокационную информацию (в том числе материалы, касающиеся сексуальных домогательств, расовых унижений, дискриминации по половому признаку, затрагивающие в оскорбительной форме вопросы возраста или сексуальной ориентации, религиозные или политические пристрастия, национальность или состояние здоровья, нарушающие законодательство РФ);

несанкционированное распространение информации рекламного характера;

использовать специальные программные средства обеспечения анонимности доступа в Интернет;

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

* 1. Пользователи при работе в Интернет должны самостоятельно обеспечивать конфиденциальность информации Предприятия, доступ к которой они получили.
  2. Любые сообщения, кроме официальных публикаций Предприятия, размещаемые Пользователями в публичный доступ в Интернет, должны включать ссылку о том, что выраженная точка зрения является личной, и не может быть расценена как официальная позиция Предприятия.

# Предоставление, изменение и прекращение полномочий доступа

* 1. Обращения по предоставлению или изменению доступа для Пользователей должны согласовываться уполномоченными работниками Предприятия, которые в свою очередь должны проанализировать обоснованность предоставления доступов.
  2. Обращения по предоставлению, изменению и блокировке доступа должны быть согласованы ЭБ Предприятия. При рассмотрении обращений уполномоченные работники ЭБ Предприятия имеют право запросить и получить любую необходимую информацию по обращению, а также отклонить обращение без обоснования причин.
  3. Предприятие имеет право в любой момент ограничить либо заблокировать доступ как отдельным Пользователям Контрагента, так и всем Пользователям Контрагента.

# Ответственность за нарушения Требований в области информационной безопасности

* 1. Несоблюдение Контрагентом/Пользователями настоящих Требований дает Предприятию право требовать от Контрагента уплаты штрафа в соответствии с указанным в настоящем пункте перечнем штрафных санкций за нарушения Требований путем перечисления подлежащей уплате суммы штрафа на расчетный счет Предприятия в течение 10 (десяти) рабочих дней с момента направления письменного обращения Предприятием. В случае невыплаты Контрагентом таких штрафов в указанный срок сумма, подлежащая оплате Контрагентом по любом договору, заключенному между Предприятием и Контрагентом, может быть уменьшена Предприятием на сумму всех штрафов и неустоек, а также иных сумм, предъявленных Предприятием в претензиях. Размер штрафа определяется исходя из нижеуказанных данных таблицы.

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Наименование нарушения, за каждый факт совершения которого Контрагент уплачивает Предприятию штраф** | **Размер штрафа, тыс. руб.** |
| 1 | Нарушение соблюдения Требований информационной безопасности в Корпоративной сети Предприятия | 150 |
| 2 | Нарушение Требований по обеспечению конфиденциальности паролей | 50 |
| 3 | Нарушение Требований по антивирусной безопасности | 50 |
| 4 | Нарушение требований по использованию ресурсов сети Интернет | 50 |

|  |  |
| --- | --- |
| АО «НИПИГАЗ» | ООО «НПФ «Технотранс» |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / Гиоргадзе Ш.А. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / Кукало П.М. |