**Приложение № 6**

к Договору от «\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ г. № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Перечень нарушений**

требований ИБ при работе на объектах Заказчика

|  |  |
| --- | --- |
| № | Описание нарушения |
| 1 | Передача информации, составляющей коммерческую тайну, либо иных конфиденциальных сведений Заказчика по незащищенным каналам передачи данных и через сеть «Интернет» способом, отличным от согласованного с Заказчиком. |
| 2 | Отсутствие ограничительного грифа на документах (проектах документов), разрабатываемых Исполнителем в рамках исполнения настоящего договора/соглашения, как на бумажных, так и машинных носителях информации в случае наличия в документе (проекте документа), сведений, составляющих коммерческую тайну Заказчика, либо иных конфиденциальных сведений. |
| 3 | Несанкционированное Заказчиком копирование и (или) модификация и (или) уничтожение (удаление) информации Заказчика. |
| 4 | Внесение пароля привилегированной (технологической) учетной записи в открытом виде в программное обеспечение, а также в настройки программного обеспечения и/или оборудования Заказчика. |
| 5 | Присвоение учетной записи пустого пароля или пароля, не соответствующего требованиям парольной политики Заказчика , а также сохранение пароля по умолчанию, заданного производителем программного обеспечения и/или оборудования после подключения (установки) его в ЛВС Заказчика. |
| 6 | Запись, хранение и/или использование при работе на АРМ ЛВС Заказчика любого дополнительного программного обеспечения (ПО), без согласования с подразделениями ИТ и ИБ Заказчика. |
| 7 | Подключение к АРМ (серверу, сетевому и прочему оборудованию) или к ЛВС Заказчика любого оборудования, без письменного согласования с подразделениями ИТ и ИБ Заказчика. |
| 8 | Загрузка АРМ (сервера, сетевого и прочего оборудования) с внешних машинных носителей информации\* (CD/DVD, USB-накопителя или других). |
| 9 | Несанкционированное изменение программного обеспечения, а также настроек программного обеспечения и/или оборудования Заказчика, в том числе создание механизма для несанкционированного отключения и/или обхода средств защиты и контроля. |
| 10 | Вскрытие АРМ (сервера, сетевого и прочего оборудования) Заказчика, внесение изменений в их конфигурацию\*. |
| 11 | Отключение антивирусного ПО или иных средств обеспечения безопасности информации\*. |
| 12 | Вирусное заражение автоматизированных рабочих мест (серверов, сетевого и прочего оборудования) Заказчика вследствие несанкционированного отключения (изменения настроек) антивирусного ПО. |
| 13 | Получение несанкционированного доступа к информационным ресурсам Заказчика, в том числе:   * предоставление своих учетных записей для работы с информационными ресурсами Заказчика (в том числе пароля и/или ключевой информации) лицам, неуполномоченным Заказчиком, * использование работниками Исполнителя, Соисполнителей для организации работы с информационными ресурсами Заказчика чужих учетных записей (в том числе пароля и/или ключевой информации);   успешная, либо безуспешные попытки подбора пароля чужой учетной записи\* |
| 14 | Использование недокументированных свойств и ошибок в программном обеспечении или в настройках средств защиты Заказчика, которые могут привести к нарушению их штатной работы, повышению полномочий пользователя или несанкционированному доступу к данным.\* |
| 15 | Использование программного обеспечения и/или оборудования Заказчика с целью извлечения Исполнителем (Соисполнителем) и/или их работниками дохода, не связанного с выполнением договора между Заказчиком и Исполнителем (в том числе для создания (майнинга) новых блоков криптовалют). |
| 16 | Действия Исполнителя в сети Интернет, совершенные с использованием ИТ-инфраструктуры Заказчика и компрометирующие Заказчика, в том числе, любые противоправные, а также могущие нанести репутационный ущерб действия   * рассылка информации (спама[[1]](#footnote-1)) от лица Заказчика; * рассылка фишинговых[[2]](#footnote-2) писем\*\*, * создание сайтов, несанкционированное Заказчиком; * несанкционированное Заказчиком изменение функциональности сайтов и других информационных ресурсов Заказчика, размещенных в сети Интернет\*\*; * вирусные заражения\*\*; * попытки несанкционированного доступа к информационным ресурсам\*\*; * нанесение ущерба информационной инфраструктуре и/или процессам\*\*; * мошенничество\*\*; * обход блокировок, установленных в соответствии с законодательством Российской Федерации и других государств;   размещение или просмотр порнографических материалов, а также материалов содержащих политическую, религиозную, социальную, экстремистскую и прочую агитацию\*\*. |
| 17 | Нарушение режима коммерческой тайны Заказчика путем привлечения Исполнителем, Соисполнителем к оказанию услуг по договору с Заказчиком третьих лиц (юридических или физических) без письменного предварительного согласия Заказчика, а также создание юридическим или физическим лицам, не являющихся соисполнителями по договору, условий для ознакомления со сведениями Заказчика, относящимся к «конфиденциальным» или к «коммерческой тайне». |

\* За исключением случаев, когда данные работы предусмотрены по договору и проводятся по согласованию и в присутствии представителя подразделения ИТ Заказчика.

\*\* За исключением случаев, подпадающих под действие ст. 272, 273, 274 и 274.1 Уголовного кодекса Российской Федерации от 13.06.1996 N 63-ФЗ.

1. Спам - массовая рассылка корреспонденции рекламного или иного характера лицам, не выражавшим желания её получать. [↑](#footnote-ref-1)
2. Фишинг – вид компьютерного мошенничества, основная цель которого обманным путем (как правило, направлением поддельного письма с вредоносной ссылкой) вынудить жертву запустить вредоносное приложение или обратиться на зараженный ресурс, что в последующем ведет к краже паролей, утечке конфиденциальной информации, заражению компьютера вирусами, шифрованию информации и др. [↑](#footnote-ref-2)