Приложение № 1
к Приказу АО «Интеркомп»
от 07 июля 2022 года № ПР-2022-0316

ПОЛОЖЕНИЕ О СОБЛЮДЕНИИ ТРЕБОВАНИЙ КИБЕРБЕЗОПАСНОСТИ

Настоящее Положение о соблюдении требований кибербезопасности (далее – «Положение») является неотъемлемой частью договора (далее – «Договор») между юридическим лицом/индивидуальным предпринимателем (далее – «Контрагент») и Акционерным обществом «Интеркомп» (далее - «СберРешения»), далее совместно именуемые – «Стороны».
Контрагент принимает все условия Положения посредством подписания Соглашения о кибербезопасности (далее – «Соглашение о КБ») или Договора, содержащего условия о присоединении Контрагента к Положению.
Реквизиты Сторон указываются в Соглашении, заключенном Сторонами к Положению, или в Договоре.
Стороны согласовали следующие условия:

- Стороны пришли к соглашению, что в течение срока действия Договора СберРешения вправе осуществлять контроль за соблюдением Контрагентом требований кибербезопасности, установленных Положением. Данный контроль осуществляется СберРешения путём направления в адрес Контрагента анкеты по форме СберРешения, которую Контрагент обязан заполнить и направить в адрес СберРешений в течение 10 (десяти) рабочих дней с момента направления. Анкета направляется по электронной почте на адрес, указанный в Соглашении о КБ;
- Подключение любых устройств, обладающих функционалом по обработке информации (включая ввод, хранение, отображение, поиск, передачу, коммутацию, управление), которые могут быть подключены к средствам вычислительной техники Группы компаний «СберРешения» по интерфейсам (включая беспроводные), предназначенным для передачи данных (далее – «Оборудование») Контрагента к ИТ-инфраструктуре СберРешений допускается только в целях исполнения обязательств по Договору в соответствии с установленными локально нормативными актами СберРешений. Контрагент обязан письменно согласовать данное подключение с ответственными лицами со стороны СберРешений, указанными в Соглашении о КБ. Подключаемое Оборудование должно соответствовать требованиям СберРешений.
- Контрагент не обрабатывает данные клиентов или партнеров СберРешений в своей информационной инфраструктуре, если иное напрямую не предусмотрено Договором.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Контрагент гарантирует, что исполнение условий Договора не приведет к появлению скрытых функциональных возможностей (недокументированных изменений, операций, либо внедренных «программных закладок»), а также компьютерных вирусов, троянов, самоликвидирующихся механизмов, механизмов защиты от копирования и других подобных машинных команд, которые могут деактивировать, уничтожить или иным образом изменить данные СберРешений, программное или аппаратное обеспечение СберРешения.

1.2. Контрагент обязуется на постоянной основе, не реже одного раза в два года, проводить внешние аудиты кибербезопасности. К проведению аудита допускаются компании, обладающие правом проведения аудитов на законном основании.

1.3. Контрагент на постоянной основе, не реже одного раза в год, должен проводить сканирование защищенности внешнего периметра локальной вычислительной сети (далее – «ЛВС») с привлечением внешних организаций, обладающих правом проведения таких работ на законном основании, при этом область сканирования должна включать, как минимум, средства вычислительной техники (далее – «СВТ») и сетевое оборудование:

- взаимодействующее с инфраструктурой СберРешений;
- сетевой траффик с которыми разрешен для автоматизированной системы (далее – «АС») или СВТ, обрабатывающих данные клиентов или партнеров СберРешений.

1.4. В случае выявления по результатам сканирования уязвимостей, эксплуатация которых потенциально несет угрозу данным клиентов СберРешений, Контрагент обязан в течение максимально короткого срока устранить данные уязвимости, а в случае невозможности устранения – незамедлительно информировать об этом СберРешения.

1.5. Запрещается организация информационного взаимодействия между Контрагентом и СберРешения по сетевым протоколам без использования шифрования трафика.

1.6. Способ организации защищенного удаленного доступа к информационным ресурсам СберРешений, технические параметры подключения, тип и настройки оборудования, используемого для удаленного доступа, определяются СберРешениями.

1.7. При организации VPN-туннеля между информационными инфраструктурами СберРешений и Контрагента должны выполняться следующие требования:

- подключение Контрагента к инфраструктуре СберРешений осуществляется путем установки сетевого соединения СВТ Контрагента с СВТ внешней сети СберРешений с обязательной трансляцией IP-адресов на сетевом оборудовании Контрагента в диапазон адресов, выданный СберРешениями и закрепленным за Контрагентом; защита соединения в этом случае реализуется с помощью средств криптографической защиты информации;
- использование технологии remote access VPN допускается только для подключения Контрагента к инфраструктуре СберРешений с использованием виртуальных АРМ СберРешений.

1.8. Если условия Договора включают разработку, модификацию, адаптацию, внедрение и техническую поддержку программного обеспечения (далее –«ПО») СберРешений, а также приобретения СберРешениями исключительного права на ПО, то результатом исполнения таких условий по Договору не будет создание нового ПО, используемого на условиях открытых лицензий (free and open-

source software), условия которых требуют от пользователя раскрытия исходного кода модифицированного ПО, либо ограничивают право пользователя запрещать третьим лицам использование модифицированного ПО. Под ПО СберРешений в рамках Положения понимается ПО, исключительное право на которое принадлежит СберРешения на момент заключения Договора и/или возникает (переходит) у СберРешений в результате надлежащего исполнения Договора.

1.9. Если условия Договора включают выполнение работ/оказание услуг по техническому обслуживанию и поддержке Оборудования/СВТ СберРешений, не подключенного к ЛВС СберРешений, Контрагент несет ответственность за своевременное обновление системного и прикладного ПО такого Оборудования/СВТ СберРешений.

1.10. Если условия Договора включают разработку, модификацию, адаптацию, внедрение ПО СберРешений, к договору на техническую поддержку (сопровождение) ПО СберРешений, текст договора которого предусматривает предоставление новой версии ПО/модификацию исходного кода ПО СберРешений с последующим проведением приемо-сдаточных испытаний и приемкой ПО СберРешений, а также приобретения СберРешениями права на ПО, то Контрагент обязуется передавать поставляемое, разрабатываемое, дорабатываемое (модифицируемое, адаптируемое) в интересах СберРешений ПО перед сдачей-приемкой работ по договору СберРешениям для тестирования и приемки с участием специалистов СберРешений. При отрицательном результате прохождения тестирования или приемки ввод ПО в эксплуатацию запрещен, работа считается невыполненной и акт приема-сдачи работ не подписывается. В целях проведения тестирования и приемки эталонный дистрибутив и исходные коды ПО (в случае передачи исходных кодов ПО в соответствии с условиями соглашения между Сторонами) передается на хранение СберРешениям до проведения приемки.

В случае если СберРешения сочтет необходимым, с исходных кодов на Оборудовании СберРешений в присутствии Контрагента проводится контрольная компиляция ПО. В случае если исходные коды ПО не передаются, после проведения контрольной компиляции осуществляется удаление исходных кодов ПО с Оборудования СберРешений. В отдельных случаях, если СберРешения сочтет необходимым, может применяться процедура депонирования исходных кодов, регулируемая отдельным соглашением СберРешений и Контрагента.

1.11. В случае, если условия Договора включают право привлечения Контрагентом третьих лиц, то соблюдаются следующие условия:

- привлечение третьих лиц Контрагент обязан предварительно письменно согласовать с СберРешениями;
- привлекаемые третьи лица обязаны соблюдать все требования Положения;
- запрещено самостоятельное подключение Контрагентом третьих лиц к ИТ-инфраструктуре СберРешений и/или предоставление доступа к СВТ и АС СберРешений без письменного согласования с СберРешениями;
- доступ работников Контрагента к СВТ СберРешений, содержащим сведения, относимые к конфиденциальной информации, в рамках Договора не предоставляется. В случае необходимости передачи привлеченному третьему лицу защищаемой информации порядок такой передачи, условия передачи и обработки, требования к защите информации определяются отдельным договором между СберРешениями и привлеченным третьим лицом;
- Контрагент несет полную ответственность за все действия и/или бездействия привлекаемых ими третьих лиц.

2. ОБЯЗАТЕЛЬСТВО О СОБЛЮДЕНИИ ТРЕБОВАНИЙ КИБЕРБЕЗОПАСНОСТИ

2.1. В случае, если в ходе сотрудничества СберРешений и Контрагента работнику Контрагента потребуется доступ к АС, Оборудованию, СВТ и в помещения (на объекты, территорию) СберРешения, работник Контрагента обязуется соблюдать требования, изложенные ниже.

2.2. Использовать предоставленный доступ к АС СберРешений, Оборудованию, СВТ и помещениям СберРешений исключительно в целях исполнения обязательств по заключенного с СберРешениями Договора.

2.3. Не разглашать и не использовать в личных целях и целях третьих лиц конфиденциальную информацию СберРешений, доступ к которой предоставлен для исполнения Договора, соблюдать конфиденциальность информации СберРешений.

2.4. Не обсуждать на форумах и в конференциях сети Интернет вопросы, касающиеся моей профессиональной деятельности в части отношений с СберРешениями и его работниками.

2.5. Препятствовать ознакомлению посторонних лиц с конфиденциальными документами СберРешений, не допускать утрату (кражу, порчу, утерю) материальных носителей (USB-носителей, оптических дисков, внешних жестких дисков и др.), содержащих конфиденциальную информацию СберРешений.

2.6. Не хранить конфиденциальную информацию СберРешений в общедоступных ресурсах, не передавать ее за пределы сетей СберРешений в открытом (незащищенном от доступа посторонних лиц) виде, не использовать для передачи конфиденциальной информации общедоступные интернет-мессенджеры (Viber, WhatsApp, Telegram, Skype и т.д.).

2.7. Без лишней необходимости не распечатывать электронные конфиденциальные документы СберРешений, забирать свои распечатанные документы из принтеров сразу после окончания печати и удалять файлы из папок сканирования.

2.8. По завершению использования, уничтожать документы и медиа-носители, содержащие конфиденциальную информацию, методом механической переработки с помощью уничтожителей бумаг (шредеров).

2.9. Оставляя рабочее место, блокировать его (комбинацией Win+L для систем под управлением Windows или Command+Control+Q для систем с Mac OS).

2.10. Не прерывать сканирование антивирусным ПО съемных машинных и медиа носителей информации (USB-носителей, оптических дисков, внешних жестких дисков и др.) при их подключении к АРМ, включенному в сеть СберРешений.

2.11. Соблюдать парольную политику в части удовлетворения следующим требованиям:

- длина пароля должна быть не менее 12 символов;
- пароль должен содержать в себе символы как минимум трех категорий из четырех: буквы нижнего регистра (от a до z), буквы верхнего регистра (от A до Z), цифры (от 0 до 9) и спецсимволы (например: $, #, %);

- пароль не должен совпадать с логином и повторять предыдущие 5 пароля для данной учетной записи пользователя;
- пароль не должен включать осмысленные слова, словосочетания, общепринятые аббревиатуры, а также основываться на доступных данных о пользователе (фамилии, дате рождения, именах родственников, номеров телефонов и др.) или легко угадываемом алгоритме смены (Smi1le!, Smi2le!, Smi3le! и т.д.);
- пароль не должен содержать широко известные или легко угадываемые слова и последовательности символов (12345678, password, qwerty, aaabbb и т.д.);
- пароль по умолчанию (созданный при создании учетной записи пользователя) должен быть изменен пользователем при первом входе;
- пароль должен изменяться не реже чем 1 раз в 30 дней с момента последнего изменения;
- в случае разглашения или компрометации пароль должен быть незамедлительно изменен.

2.12. Соблюдать правила обращения с паролями:
- не записывать пароль на предметах и материальных носителях, а также не хранить его в файле в открытом виде;
- не использовать один и тот же пароль для различных учетных записей;
- не передавать кому-либо (в т.ч. своим коллегам и руководителям, а также работникам СберРешений) свой пароль, равно как и использовать чужие пароли для работы с СВТ и АС СберРешений;
- не осуществлять попытки подбора паролей (в том числе автоматизированными способами), не пытаться завладеть паролями других лиц.

2.13. Не организовывать на предоставленном компьютере ресурсы общего доступа и сетевые сервисы (открывать доступ к общим папкам, дискам, CD-приводам и дисководам, настраивать службы удаленного доступа, прокси- или веб-серверы, беспроводные точки доступа, Bluetooth интерфейсы и т.д.).

2.14. Не предпринимать попытки преодоления установленных СберРешениями ограничений, отключать и/или удалять установленные на предоставленных СВТ СберРешений средства защиты информации (в том числе антивирусное программное обеспечение), использовать недокументированные свойства, ошибки в программном обеспечении и настройках защиты доступа к информационным ресурсам и АС СберРешений, доступ к которым не был предоставлен явным образом.

2.15. Не устанавливать на предоставленные СВТ СберРешений какое-либо программное обеспечение, изменять настройки уже имеющегося. По вопросам установки необходимого программного обеспечения, а также получения административных прав в операционных системах персональных компьютеров обращаться в отдел информационных технологий СберРешений.

2.16. Не хранить и не использовать на предоставленном компьютере программное обеспечение, фонограммы и другие результаты интеллектуальной деятельности в нарушение прав их законных правообладателей.

2.17. Не открывать вложения и не переходить по ссылкам, указанным в почтовых сообщениях, имеющих признаки фишинга, включая:
- сообщение замаскировано под официальное письмо организации и требует каких-либо быстрых действий или ответа;
- сообщение содержит ссылки на Интернет-ресурсы, визуально похожие на оригинальные ресурсы организации, однако в отношении которых возникают сомнения;
- к сообщению прикреплен файл-вложение, который настойчиво предлагается открыть;
- в тексте сообщения содержатся опечатки, ошибки, избыточные знаки препинания.

2.18. Не переходить по коротким ссылкам вида bit.ly или goo.gl.

2.19. Не вскрывать корпус предоставленного компьютера (в том числе для самостоятельного устранения неисправностей), самовольно подключать к нему какое-либо оборудование (GPRS модемы, Wi-Fi точки доступа и пр.).

2.20. Не подключать к предоставленным СВТ СберРешений личные мобильные устройства (телефоны, смартфоны, планшетные компьютеры, ноутбуки), беспроводные (радио) интерфейсы, модемы и прочее оборудование, позволяющее выходить в сеть Интернет и другие публичные сети.

2.21. Не использовать без письменного согласования программное обеспечение следующих категорий при подключении к корпоративной сети СберРешений:
- сканеры портов и анализаторы трафика;
- средства для организации удаленного доступа, не утвержденные требованиями СберРешений, включая средства для создания зашифрованных каналов связи (VPN-, DNS-, SSH-, HTTPS-туннели и пр.);
- ПО, используемое для анонимного доступа в сеть Интернет (включая веб-сервисы, прокси-серверы);
- ПО для обхода средств защиты, включая средства подбора и восстановления паролей, поиска уязвимостей;
- ПО, предназначенное для сокрытия или внедрения дополнительной информации в цифровые объекты (в том числе реализующее методы стеганографии);
- ПО, осуществляющее сбор информации с клавиатуры, экрана, микрофона (снифферы);
- специализированные программные средства, оказывающее влияние на сетевые настройки СВТ, серверов и сетевого оборудования.

2.22. Не рассылать с корпоративных почтовых адресов СберРешений сообщений развлекательного, рекламного и иного характера, не относящегося к оказанию услуг по Договору.

2.23. Не использовать АРМ СберРешений (в том числе с использованием расширений к web-браузеру) и личные СВТ, подключенные к сетям СберРешений, для посещения Интернет-ресурсов:
- содержание и направленность которых запрещены международным и российским законодательством;
- содержащих материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц;
- содержащих материалы, способствующие разжиганию межнациональной розни, подстрекающие к насилию, призывающие к

совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия и т.д.

2.24. Не оставлять без присмотра или передавать кому-либо предоставленные пропуска и прочие средства идентификации, а также ключи от помещений СберРешений.

2.25. По требованию уполномоченных представителей СберРешений предоставлять выданные СВТ СберРешений и носители информации (USB-Flash, CD/DVD и др.) для проверки выполнения требований информационной безопасности.

2.26. Информировать ответственное лицо СберРешений по вопросам кибербезопасности обо всех инцидентах КБ (обоснованных подозрениях на инцидент) и событий, создающих угрозу причинения ущерба СберРешениям, а также об обращениях третьих лиц с целью незаконного получения конфиденциальной информации СберРешений.

2.27. СберРешения вправе контролировать действия Контрагента при работе с АС СберРешений, оборудованием и средствами вычислительной техники, включая анализ отправленных информационных сообщений, в т.ч. с использованием корпоративных почтовых систем СберРешений и с использованием сети Интернет.

2.28. СберРешения вправе использовать полученную в результате такого анализа информацию для проведения расследований, в том числе, с привлечением правоохранительных органов, а также использовать в качестве доказательств в суде, в этих случаях Контрагент не вправе рассчитывать на соблюдение в отношении этих сообщений конфиденциальности со стороны СберРешений.

2.29. В случае выявления нарушений перечисленных требований, повлекших причинение ущерба СберРешениям, СберРешения вправе отстранить Контрагента от работ, приостановить доступ к своим АС, оборудованию, СВТ и в помещения СберРешений, а в случае подтверждения факта ущерба, требовать его возмещения от Контрагента я, в т.ч. в судебном порядке.

3. ОБМЕН ИНФОРМАЦИЕЙ ОБ ИНЦИДЕНТАХ КИБЕРБЕЗОПАСНОСТИ

3.1. В целях оперативного взаимодействия Стороны определяют сотрудников, ответственных за обмен информацией о значимых инцидентах (подозрениях на инциденты) КБ и указывают их в Соглашении о КБ (далее – «Ответственный»).

3.2. Контрагент обязан информировать СберРешений обо всех фактах нарушения требований Положения или событиях, способных привести к таким нарушениям. Информирование осуществляется в максимально короткий срок, но не позднее 24 часов с момента обнаружения данного факта через Ответственного со стороны СберРешений.

3.3. При возникновении в инфраструктуре Контрагента значимого инцидента КБ, последствия которого могут затронуть интересы СберРешений (в том числе клиентов или партнеров СберРешений), Контрагент обязан известить об этом СберРешения в максимально возможный короткий срок, но не позднее 8 (восьми) часов с момента обнаружения такого инцидента (подозрения на инцидент).

3.4. Значимым считается инцидент КБ, удовлетворяющий одному из следующих критериев:

- невозможность выполнения СберРешениями бизнес-операций, в соответствии с установленными сроками для структурного подразделения, или ограничение функциональности ИТ-услуги или АС;
- разглашение аутентификационных данных или конфиденциальной информации (в том числе персональные данные);
- воздействие вредоносного программного обеспечения (далее – «ВПО»), массовые блокировки учетных записей, создание несанкционированных учетных записей;
- выявленные признаки несанкционированного доступа (далее – «НСД») или неудачных попыток получения НСД, а также злоупотребление привилегиями.

3.5. В перечень инцидентов КБ Стороны включают инциденты, несущие риски потери конфиденциальности, целостности, доступности информации, в том числе:

- фишинговая атака якобы от имени Стороны;
- эксплуатация выявленной уязвимости на ресурсе, принадлежащем Стороне;
- эксплуатация выявленной уязвимости в ПО, предоставляемом/эксплуатируемом Стороной;
- заражение ВПО;
- НСД к ресурсам Стороны;
- DDOS-атака на ресурсы Стороны – выявленная, закончившаяся или планируемая.

3.6. В случае устранения значимого инцидента КБ Контрагент обязан уведомить СберРешения о мерах, предпринятых для управления инцидентом в течение 24 часов.

3.7. Стороны обмениваются информацией об инцидентах в свободном формате. Для повышения оперативности при передаче технической информации Стороны вправе использовать телефонную связь и иные каналы передачи информации.

3.8. В рамках обмена информацией об инцидентах КБ Стороны не обмениваются информацией, содержащей персональные данные и иную информацию ограниченного доступа.

3.9. В случае появления новых типов инцидентов КБ, способов и механизмов их выявления, а также при необходимости оптимизации взаимодействия или изменения форматов передаваемых файлов, в Соглашение по взаимному согласованию Сторон вносятся необходимые изменения (дополнения).

4. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

4.1. Контрагент обязуется ознакомить своих работников с требованиями Положения.

4.2. Контрагент несет ответственность за действия своих работников, выполняющих работы (оказывающих услуги) в АС, на Оборудовании, СВТ и в помещениях СберРешений в полном объеме.

4.3. В случае нарушения Контрагентом требований Положения, как существенного условия Договора, СберРешения вправе отказать Контрагенту в предоставлении доступа к своей ИТ-инфраструктуре, оказании услуг, а также отказаться от Договора в любое время без возмещения убытков Контрагенту, путём направления Контрагенту соответствующего уведомления не менее чем за 5 (пять)

рабочих дней до момента прекращения Договора.

4.4. В каждом случае нарушений требований Положения, Контрагент выплачивает СберРешениям штрафную неустойку в размере 10 (десять) % от общего размера вознаграждения, указанного в Договоре, а также обязуется в полном объёме возместить убытки, причинённые СберРешениям вследствие нарушения Контрагентом положений Соглашения и Положения. Взыскание убытков не лишает СберРешения возможности прибегать к любым иным мерам защиты своих прав и интересов, предусмотренных действующим законодательством Договором, в том числе взысканию неустойки в полном размере сверх убытков.

4.5. В каждом случае нарушения требований Положения, повлекшего возникновение значимого инцидента КБ в ИТ-инфраструктуре СберРешений или наступления события на стороне Контрагента, повлекшего возникновение значимого инцидента КБ в ИТ-инфраструктуре СберРешений, Контрагент обязан выплатить СберРешениям штрафную неустойку в размере 10 (десять) % от общего размера вознаграждения, указанного в Договоре, за каждый инцидент, а также полностью возместить причиненные ему убытки.

4.6. В случае нарушения Контрагентом принятых на себя обязательств по Соглашению и Положению, Контрагент обязуется возместить СберРешениям убытки, причиненные таким нарушением. Убытки возмещаются в соответствии с законодательством Российской Федерации. Кроме того, в случае, если к СберРешениям будут предъявлены претензии (требования, иски) со стороны третьих лиц и/или государственных органов, вследствие реализованных рисков кибербезопасности, в рамках Соглашения или Положения, Контрагент по получении извещения от СберРешений обязуется а) выступить на стороне СберРешений, б) оказать всемерное содействие СберРешениям при урегулировании таких претензий, в том числе в) взять на себя обязанность по подготовке и проведению досудебных переговоров и переписки с такими третьими лицами или государственными органами, а впоследствии (в том случае, если СберРешения будет вынуждено в силу вступившего в силу решения суда или если по согласованию с Контрагентом будет признано приемлемым возместить ущерб третьих лиц во внесудебном порядке) г) возместить СберРешениям в полном объеме выплаченные СберРешениями третьим лицам или государственным органам денежные средства, связанные с нарушением прав третьих лиц судебные издержки СберРешений и иные расходы. Возмещение производится Контрагентом не позднее 10 (десяти) рабочих дней со дня получения соответствующего письменного требования и счета от СберРешений.

4.7. СберРешения вправе пересмотреть условия Положения по своей инициативе в следующих случаях:

- наличие у СберРешений необходимости сохранить надлежащий уровень контроля и управления в отношении риска нарушения КБ Контрагентом;
- наличие у СберРешений необходимости принять соответствующие меры для выполнения своих обязательств перед клиентами и контрагентами, а также уполномоченными государственными органами.

4.7. Все споры, разногласия и требования, возникающие из Положения или в связи с ним, в том числе касающиеся его исполнения, нарушения, прекращения или недействительности, будут разрешаться Сторонами претензионным путем. В случае если одна Сторона посчитает, что ее право нарушено, она должна направить другой Стороне обоснованную письменную претензию.

4.8. Сторона, получившая претензию, обязана удовлетворить ее, либо направить мотивированные возражения в срок не более 10 (десяти) рабочих дней с момента получения претензии.

4.9. В случае, если претензия одной Стороны не удовлетворена и мотивированные возражения не получены, либо полученные мотивированные возражения не считаются Стороной, право которой нарушено, обоснованными, споры подлежат разрешению в Арбитражном суде г. Москвы.