ТРЕБОВАНИЯ ПО КИБЕРБЕЗОПАСНОСТИ¹

- 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 Общества, программное или аппаратное обеспечение Общества.
- 1.2 Если условия Договора включают выполнение работ/оказание услуг по техническому обслуживанию и поддержке Оборудования/СВТ/инфраструктуры Общества, Контрагент несет ответственность за своевременное обновление системного и прикладного ПО такого Оборудования/СВТ или такой инфраструктуры Общества.
- 1.3 В целях оперативного взаимодействия Стороны определяют сотрудников, ответственных за обмен информацией о значимых инцидентах (подозрениях на инциденты) КБ. При возникновении инцидента стороны обмениваются информацией в свободном формате. Для повышения оперативности при передаче технической информации Стороны вправе использовать телефонную связь и иные каналы передачи информации.
- 1.4 Контрагент обязуется на постоянной основе, не реже одного раза в два года, проводить внешние аудиты кибербезопасности.
- 1.5 К проведению аудита допускаются компании, имеющие необходимые лицензии ФСТЭК и ФСБ на осуществление деятельности в сфере информационной безопасности.
- 1.6 Контрагент на постоянной основе, не реже одного раза в год, должен проводить сканирование защищенности внешнего периметра локальной вычислительной сети 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:
 - 1.6.1 взаимодействующее с инфраструктурой Общества;
 - 1.6.2 сетевой трафик с которыми разрешен для автоматизированной системы (далее – «АС») или СВТ, обрабатывающих данные клиентов или партнеров Общества.
- 1.7 В случае выявления по результатам сканирования уязвимостей, эксплуатация которых потенциально несет угрозу данным клиентов Общества, Контрагент обязан уведомить Общество о выявленных уязвимостях и устранить их с учётом SLA по устранению уязвимостей, принятого в Обществе. В случае невозможности устранения – незамедлительно информировать об этом Общество.
- 1.8 При возникновении в инфраструктуре Общества, выполнение работ/оказание услуг по техническому обслуживанию и поддержке которой включают в себя условия Договора, значимого инцидента КБ, последствия которого могут затронуть интересы Общества (в том числе клиентов или партнеров Общества), Контрагент обязан известить об этом Общество в максимально возможный короткий срок, но не позднее 8 (восьми) часов с момента обнаружения такого инцидента (подозрения на инцидент), а о мерах, предпринятых для управления инцидентом – в течение 24 часов.
- 1.9 Значимым считается инцидент КБ, удовлетворяющий одному из следующих критериев:
 - 1.9.1 невозможность выполнения Обществом бизнес-операций, в соответствии с установленными сроками для структурного подразделения, или ограничение функциональности ИТ-услуги или АС;
 - 1.9.2 разглашение аутентификационных данных или конфиденциальной информации (в том числе персональные данные);

¹ Данные требования предъявляются к Контрагентам, которые предоставляют готовые ИТ-решения, либо занимаются созданием/эксплуатацией Систем Общества

- 1.9.3 воздействие вредоносного программного обеспечения (далее – «ВПО»), массовые блокировки учетных записей, создание несанкционированных учетных записей;
- 1.9.4 выявленные признаки несанкционированного доступа (далее – «НСД») или неудачных попыток получения НСД, а также злоупотребление привилегиями.
- 1.10 В перечень инцидентов КБ Стороны включают инциденты, несущие риски потери конфиденциальности, целостности, доступности информации, в том числе:
 - 1.10.1 фишинговая атака якобы от имени Стороны;
 - 1.10.2 эксплуатация выявленной уязвимости на ресурсе, принадлежащем Стороне;
 - 1.10.3 эксплуатация выявленной уязвимости в ПО, предоставляемом/эксплуатируемом Стороной;
 - 1.10.4 заражение ВПО;
 - 1.10.5 НСД к ресурсам Стороны;
 - 1.10.6 DDOS-атака на ресурсы Стороны – выявленная, закончившаяся или планируемая.
- 1.11 Запрещается организация информационного взаимодействия между Контрагентом и Обществом по сетевым протоколам без использования шифрования трафика.
- 1.12 Подключение любых устройств, обладающих функционалом по обработке информации (включая ввод, хранение, отображение, поиск, передачу, коммутацию, управление), которые могут быть подключены к средствам вычислительной техники Общества по интерфейсам (включая беспроводные), предназначенным для передачи данных Контрагента к ИТ-инфраструктуре Общества допускается только в целях исполнения обязательств по Договору в соответствии с установленными локально нормативными актами Общества.
- 1.13 Контрагент не обрабатывает данные клиентов или партнеров Общества в своей информационной инфраструктуре, если иное напрямую не предусмотрено Договором.
- 1.14 В случае, если условия Договора предусматривают право привлечения Контрагентом третьих лиц, то соблюдаются следующие условия:
 - 1.14.1 привлечение третьих лиц Контрагент обязан предварительно письменно согласовать с Обществом;
 - 1.14.2 запрещено самостоятельное подключение Контрагентом третьих лиц к ИТ-инфраструктуре Общества и/или предоставление доступа к СВТ и АС Общества без письменного согласования с Обществом;
 - 1.14.3 доступ работников Контрагента к СВТ Общества, содержащим сведения, относимые к конфиденциальной информации (персональные данные и иная информация ограниченного доступа), 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 Обществом и привлеченным третьим лицом;
- 1.15 Контрагент несет полную ответственность за все действия и/или бездействия привлекаемых ими третьих лиц.