

**Соглашение по информационной безопасности
при реализации типа подключения контрагента к инфраструктуре Х5
«Подключение с использованием VPN (САС) по стандартному профилю для внешних
пользователей (sslvpn.x5.ru/x5b)» (далее – Соглашение)**

г. _____

_____. _____.20__

_____, именуемое в дальнейшем «Х5», в лице уполномоченного представителя, указанного в разделе реквизиты и подписи Сторон настоящего Соглашения, с одной стороны, и

_____, именуемый в дальнейшем «КА», указанный в разделе реквизиты и подписи Сторон настоящего Соглашения, с другой стороны, заключили настоящее Соглашение к Договору № _____ от _____ (далее – договор) о нижеследующем:

1. ПРЕДМЕТ СОГЛАШЕНИЯ

1.1. В соответствии с Соглашением КА обязуется безоговорочно соблюдать требования по информационной безопасности, применению защитных мер и проведению мероприятий, перечисленных в разделах 2, 3 и 4 Соглашения.

1.2. Условия Соглашения являются обязательными для КА и распространяются на отношения Сторон, связанные с исполнением обязательств, принятых по договорам, заключенным между Сторонами, включая, но не ограничиваясь, договоры поставки, договоры о предоставлении КА для Х5 услуг по разработке, доработке (модификации, адаптации), настройке программного обеспечения (далее – ПО) и информационных систем (далее – ИС), по поддержке (сопровождению) ПО и ИС, а также договоры информационного и технологического взаимодействия.

2. ТРЕБОВАНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. В связи с необходимостью выполнения КА обязательств, предусмотренных договором, Х5 предоставляет КА доступ к следующим средствам вычислительной техники (далее - СВТ) и информационным системам Х5:

- корпоративный ноутбук;
- учётная запись в домене Х5;
- доступ к КСПД Х5 (в т.ч. по технологии VPN);
- доступ к корпоративной электронной почте Х5.

2.2. КА обязуется при реализации типа подключения КА к инфраструктуре Х5 «Подключение с использованием VPN (САС) по стандартному профилю для внешних пользователей (sslvpn.x5.ru/x5b)» соблюдать следующие требования по информационной безопасности (далее – требования по ИБ) при работе с СВТ и ИС.

2.3. Требования к защитным мерам обеспечения информационной безопасности на стороне КА:

- почтовый обмен организуется на базе электронного почтового ящика, предоставленного Х5;
- устройства КА, с которых производится подключение, должны быть оснащены функционирующим и актуальным антивирусным ПО, также должны быть установлены последние актуальные обновления операционной системы и системного ПО;
- удаленный защищенный доступ к информационным ресурсам Х5 организуется в соответствии с требованиями Х5;
- информационное взаимодействие КА с Х5 по сетевым протоколам должно быть организовано с использованием шифрования трафика.

2.4. КА обязуется не использовать СВТ и ИС Х5 в собственных целях, а также в целях:

- создания, передачи или получения сообщений, нарушающих законодательство, в т.ч. в области защиты информации, коммерческой тайны и персональных данных;
- распространения рекламы, агитации, пропаганды религиозных или политических идей;
- создания, передачи или получения сообщений с использованием не принадлежащих КА учетных записей (идентификаторов), адресов электронной почты. Разрешено использовать только учетные записи, созданные специально для выполнения работ КА;
- создания, передачи или получения вредоносных программ (вирусов, «тройных коней» и т.п.)
- передачи информации, составляющей коммерческую тайну, иной конфиденциальной информации, персональных данных, документов, содержащих указанную информацию и данные третьим лицам или на не принадлежащие Х5 ресурсы без предварительного согласования с Х5;

- умышленного или неосторожного причинения убытков Х5 или распространения сведений, порочащих деловую репутацию Х5.

2.5. КА обязуется не совершать следующие действия:

- использовать аппаратные и программные средства, позволяющие обойти ограничения, установленные настройками и правилами безопасности средствами защиты информации Х5;
- публиковать предоставленные Х5 адреса электронной почты в сети Интернет (новостные конференции, форумы и т.п.);
- отправлять сообщения размером более 35 Мбайт;
- изменять настройки программного или аппаратного обеспечения, баз данных и сетевой конфигурации рабочих станций и ИС Х5;
- устанавливать, запускать на рабочей станции, передавать в ИС или по телекоммуникационным каналам связи компьютерные игры, видеоролики и т.п., если это не предусмотрено в договоре;
- подключать без предварительного согласования с Х5 принадлежащие КА устройства к ИС Х5;
- передавать без согласия Х5 информацию, составляющую коммерческую тайну Х5, иную конфиденциальную информацию во внешние (не принадлежащие Х5) адреса ресурсов в сети «Интернет», адреса электронной почты или через общедоступные почтовые и файлообменные системы, мессенджеры и системы обмена сообщениями;
- устанавливать режим автоматической переадресации сообщений электронной почты, при работе в системе корпоративной электронной почте Х5;
- осуществлять несанкционированное чтение, модификацию, удаление чужих (т.е. не адресованных ему) сообщений электронной почты;
- модифицировать принадлежащие и/или предустановленные Х5 программы, если иное не согласовано в договоре;
- применять в электронных почтовых сообщениях приемы сокрытия информации (шифрование, архивирование, стеганография, маскирование и пр.);
- передавать предоставленные для доступа в ИС Х5 пароли и данные учетных записей;
- передавать третьим лицам каким-либо образом полученный от Х5 доступ к СВТ и/или ИС Х5, если это предварительно не согласовано с Х5 в письменной форме;
- использовать без предварительного согласования с Х5 внешние носители информации (накопители на гибких магнитных дисках, устройства CD ROM/CD RW/DVD оптические, магнитооптические накопители, USB-носители, карты памяти и т.п.) для работы с СВТ и ИС Х5.

2.6. По завершении работы заблокировать СВТ или выключить их, выйти из ИС.

3. ПРАВА И ОБЯЗАННОСТИ СТОРОН

3.1. КА обязуется ознакомиться с требованиями по ИБ, указанными в данном Соглашении, и обеспечить соблюдение этих требований. КА несет ответственность в части исполнения требований к защитным мерам обеспечения информационной безопасности, в том числе ответственность за соблюдение законодательства РФ.

3.2. КА обязуется предоставить Х5 подтверждение ознакомления (под подпись) с требованиями по ИБ в течение одного рабочего дня с даты получения соответствующего запроса со стороны Х5.

3.3. Х5 вправе вести контроль, логирование и запись действий КА.

3.4. Х5 вправе в любое время по собственной инициативе без объяснения причин произвести блокировку ранее предоставленного КА доступа.

3.5. Х5 вправе в случае нарушения КА или привлеченными им третьими лицами требований по ИБ, прекратить доступ КА к СВТ и ИС Х5.

4. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. При возникновении значимого инцидента информационной безопасности или ИТ-инцидента, последствия которого могут затронуть интересы клиентов или партнеров Х5, Стороны обязаны известить об этом друг друга в максимально возможный короткий срок, но не позднее 3-х (трех) часов с момента обнаружения такого инцидента, в порядке, описанном ниже. Значимость инцидента определяется согласно п. 4.2 Соглашения. Х5 вправе оказывать помощь КА в расследовании причин и ликвидации последствий указанного инцидента.

4.2. Значимым считается инцидент, удовлетворяющий одному из следующих критериев:

- невозможность выполнения бизнес-операций, в соответствии с установленными сроками для структурного подразделения, или ограничение функциональности ИТ-услуги или ИС для систем категории Mission Critical и Business Critical;
- разглашение аутентификационных данных или конфиденциальной информации, включая коммерческую тайну, персональные данные и иные виды информации ограниченного доступа в

соответствии с законодательством РФ;

- воздействие вредоносного кода, массовые блокировки учетных записей, создание несанкционированных учетных записей;
- выявленные признаки несанкционированного доступа (далее – НСД) или неудачных попыток получения НСД, а также злоупотребление привилегиями;
- попытки реализации угроз и атаки, предотвращённые средствами защиты информации.

4.3. В целях оперативного взаимодействия Стороны назначают ответственных за обмен данными:

- от Х5 Дежурная смена, телефон +7 (495) 662-88-88; e-mail: info-uib@x5.ru

- от КА _____

4.4. Стороны могут осуществлять обмен информацией:

- инициативно – иницилирующая Сторона направляет информацию;
- по запросу – в рамках запроса по инциденту информационной безопасности.

4.5. В случае выявления значимого инцидента информационной безопасности КА обязан уведомить Х5 в максимально возможный короткий срок, но не позднее трех часов с момента обнаружения такого инцидента.

4.6. В случае устранения значимого инцидента информационной безопасности КА обязан уведомить Х5 о мерах, предпринятых для управления инцидентом в течение 24 часов.

4.7. КА обязуется информировать Х5 обо всех факторах, связанных с возникновением риска нарушения информационной безопасности. Информация о факторе должна включать тип событий, ведущих к возникновению риска и обстоятельства их реализации.

4.8. По взаимной договоренности Стороны обмениваются информацией в свободном формате. Для повышения оперативности при передаче технической информации Стороны вправе использовать телефонную связь.

4.9. Стороны обмениваются информацией об инцидентах информационной безопасности, влияющих на исполнение договорных обязательств, выявленных с помощью информационных ресурсов Сторон, включая, но не ограничиваясь информацией о следующих типах инцидентов информационной безопасности:

- фишинговая атака якобы от имени Стороны;
- выявленная уязвимость на ресурсе, принадлежащем Стороне;
- выявленная уязвимость в ПО, предоставляемом/эксплуатируемом Стороной;
- заражение вредоносным ПО;
- попытки НСД к ресурсам Стороны;
- DDOS-атака на ресурсы Стороны – выявленные, закончившиеся и планируемые.

4.10. В случае появления новых типов инцидентов информационной безопасности, 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).

5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

5.1. Соглашение вступает в силу с момента его подписания Сторонами и действует в течение 1 (одного) года. Срок действия Соглашения продлевается на каждый последующий год, если ни одна из Сторон не уведомит в письменной форме другую Сторону о расторжении Соглашения за 30 (тридцать) календарных дней до истечения срока действия Соглашения.

5.2. Х5 вправе в одностороннем порядке пересмотреть условия Соглашения по своей инициативе в следующих случаях:

- наличие у Х5 необходимости сохранить надлежащий уровень контроля и управления в отношении риска нарушения информационной безопасности КА;
- наличие у Х5 необходимости принять соответствующие меры для выполнения своих обязательств перед клиентами и контрагентами, а также перед государственными регуляторами в области защиты информации.

5.3. Соглашение прекращает свое действие в момент прекращения Договора.

5.4. КА несет ответственность за нарушение требований по ИБ и обязан возместить Х5 причиненные нарушением указанных требований убытки в полном объеме, а также выплатить штраф в размере 100 000 рублей за каждый выявленный факт нарушения требований в течение 5 календарных дней с даты получения от Х5 соответствующего требования.

5.5. КА несет ответственность за действия и бездействие привлеченных им третьих лиц, как за свои собственные, в том числе за соблюдение такими лицами требований по ИБ. При возникновении у Х5

убытков в связи или в результате действий (бездействия) таких привлеченных лиц, КА обязан возместить Х5 причиненные убытки в полном объеме, а также выплатить штраф в размере 100 000 рублей за каждый выявленный факт нарушения требований в течение 5 календарных дней с даты получения от Х5 соответствующего требования.

5.6. Х5 вправе удержать суммы убытков, неустоек, предусмотренных Договором, из любых сумм, подлежащих уплате КА по настоящему Договору, а также по любым иным договорам, заключенным с КА.

6. РЕКВИЗИТЫ И ПОДПИСИ СТОРОН

Наименование юридического лица Юридический адрес: ОГРН ИНН	ФИО Паспорт серия номер Выдан код подразделения Зарегистрирован по адресу ИНН
Подпись и расшифровка (ФИО)	Подпись и расшифровка (ФИО)