СОГЛАШЕНИЕ О КИБЕРБЕЗОПАСНОСТИ

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. **Автоматизированная система** – совокупность взаимосогласованных компонентов программного, технического, информационного, организационного, методического, правового обеспечения, используемая пользователями для реализации заданной информационной технологии.

1.2. **Вредоносное программное обеспечение** – программное обеспечение, предназначенное для получения несанкционированного доступа к устройству пользователя или к информации, хранимой на нем, с целью несанкционированного использования информационных ресурсов или причинения вреда.

1.3. **Доступность** – гарантия того, что авторизованные пользователи могут иметь доступ и работать с необходимыми информационными активами, ресурсами и системами с требуемой производительностью.

1.4. **Информационный актив** – информация с реквизитами, позволяющими ее идентифицировать, имеющая ценность для ООО «АБТ», находящаяся в его распоряжении и представленная на любом материальном носителе в форме, пригодной для ее обработки, хранения или передачи.

1.5. **Информационный ресурс** – отдельный документ или отдельный массив документов, документ или массив документов в автоматизированной системе (библиотеке, архиве, фонде, банке/базе данных и т.д.).

1.6. **Инцидент кибербезопасности** – реализованная угроза в киберпространстве, любое непредвиденное или нежелательное событие, которое может нарушить бизнес-процесс или состояние защищенности информационного актива.

1.7. **Кибербезопасность –** обеспечение защищенности Киберпространства, в котором функционирует бизнес, достигаемое применением набора средств, методик и принципов, направленных на противодействие Угрозам кибербезопасности и минимизацию последствий от их реализации. К задачам обеспечения кибербезопасности относится, в том числе, защита всех видов сведений конфиденциального характера, определенных в соответствии с применимым законодательством, включая, но не ограничиваясь персональными данными, сведениями, составляющими банковскую или коммерческую тайну, информацию об объектах критической информационной инфраструктуры. Под применимым законодательством понимается законодательство Российской Федерации, международные нормы и законодательство стран присутствия компаний Группы, включая соответствующие нормативные правовые акты.

1.8. **Киберпространство** – информационное пространство, образованное совокупностью телекоммуникационных сетей и оборудования, средств вычислительной техники и программного обеспечения, а также деятельностью человека по его информационному наполнению.

1.9. **Коммерческая тайна** – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

1.10. **Конфиденциальность** – характеристика, определяющая, что информация не может быть доступной и раскрытой неавторизованным лицом, логическим объектом или процессом.

1.11. **Конфиденциальная информация** – информация, в отношении которой ООО «АБТ», не ввел режим коммерческой тайны, но принял меры защиты (включая меры по ограничению доступа).

1.12. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту Персональных данных).

1.13. **Передача Персональных данных** - взаимодействие, в рамках которого происходит передача Персональных данных от ООО «АБТ», к Пользователю (включая предоставление и доступ).

1.14. **Подключение** – действие, последствием которого является передача информации между Оборудованием Пользователя и инфраструктурой или СВТ ООО «АБТ».

1.15. **Средства вычислительной техники** – автоматизированные рабочие места и оргтехника (средства печати, копирования и сканирования и т.д.), а также серверное и сетевое оборудование.

1.16. **Оборудование** – любые устройства, обладающие функционалом по обработке информации (включая ввод, хранение, отображение, поиск, передачу, коммутацию, управление), которые могут быть подключены к СВТ ООО «АБТ» по интерфейсам (включая беспроводные), предназначенным для передачи данных.

1.17. **Объект защиты** – элемент ИТ-инфраструктуры или набор элементов, объединенных определенным функциональным качеством (АРМ, сервер, АС, платформа, сетевое оборудование, сегмент сети, домен, группа доменов, ИТ-сервис и пр.).

1.18. **Угроза кибербезопасности** – совокупность условий и факторов, создающих потенциально или реально существующую опасность нарушения кибербезопасности в отношении Объекта зашиты.

1.19. **Уязвимость** – недостаток в компьютерной системе, использование которого приводит к нарушению целостности системы и некорректной работе.

1.20. **Целостность** – свойство сохранения правильности и полноты информационных активов ООО «АБТ».

2. СОКРАЩЕНИЯ

2.1.	**DDOS**	Distributed Denial of Service (атака типа «распределенный отказ в обслуживании»)
2.2.	**АС**	Автоматизированная система
2.3.	**АРМ**	Автоматизированное рабочее место
2.4.	**ВПО**	Вредоносное программное обеспечение
2.5.	**ИР**	Информационный ресурс
2.6.	**КБ**	Кибербезопасность
2.7.	**НСД**	Несанкционированный доступ
2.8.	**РФ**	Российская Федерация
2.9.	**СВТ**	Средства вычислительной техники

3. ПРЕДМЕТ СОГЛАШЕНИЯ

3.1. В соответствии с Соглашением Пользователь обязуется безоговорочно соблюдать требования по кибербезопасности, применять защитные меры и проводить мероприятия, перечисленные в разделах 4 и 5 Соглашения. Условия Соглашения являются обязательными для Пользователя и распространяются на отношения Сторон, связанные с исполнением обязательств, принятых по договорам, заключенным между Сторонами, включая, но не ограничиваясь, договорами поставки, договорами о предоставлении Пользователем Правообладателю услуг по разработке, доработке (модификации, адаптации), настройке ПО и АС, по поддержке (сопровождению) ПО и АС, а также договорами информационного и технологического взаимодействия.

3.2. Стороны признают, что обязательство Пользователя по исполнению требований по кибербезопасности, применению защитных мер, проведению мероприятий и иных условий, установленных Соглашением, является обстоятельством, имеющим существенное значение для ООО «АБТ» для заключения, исполнения и прекращения договоров, указанных в п. 3.1 Соглашения (по смыслу п. 2 ст. 431.2 Гражданского кодекса РФ).

4. ТРЕБОВАНИЯ ПО КИБЕРБЕЗОПАСНОСТИ

4.1. Стороны обязуются обеспечить наличие между ними, к моменту заключения Соглашения, действующего соглашения о неразглашении конфиденциальной информации, заключенного по форме, предложенной ООО «АБТ».

4.2. Запрещается информационное взаимодействие между Пользователем и ООО «АБТ» по сетевым протоколам без использования шифрования трафика. Взаимодействие посредством электронной почты организуется в соответствии с п. 4.4 Соглашения.

4.3. Удаленный доступ к информационной инфраструктуре ООО «АБТ» Пользователю не предоставляется.

4.4. Почтовый трафик между ООО «АБТ» и Пользователем должен передаваться с использованием шифрования; при использовании протокола TLS должна использоваться версия не ниже 1.1.

5. ОБМЕН ИНФОРМАЦИЕЙ ОБ ИНЦИДЕНТАХ КИБЕРБЕЗОПАСНОСТИ

5.1. При возникновении в инфраструктуре Пользователя значимого инцидента КБ, последствия которого могут привести к утрате целостности, доступности или конфиденциальности данных, обрабатываемых в рамках настоящего Договора, Пользователь обязан известить об этом ООО «АБТ» в максимально возможный короткий срок, но не позднее 3-х (трех) часов с момента обнаружения такого инцидента (подозрения на инцидент).

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

5.2.1. невозможность выполнения бизнес-операций, в соответствии с установленными сроками для структурного подразделения Лицензиата, или ограничение функциональности ИТ-сервиса или АС;

5.2.2. разглашение аутентификационных данных или конфиденциальной информации (коммерческая тайна, банковская тайна, персональные данные, иное);

5.2.3. воздействие ВПО, массовые блокировки учетных записей, создание несанкционированных учетных записей;

5.2.4. выявленные признаки НСД или неудачного получения НСД, а также злоупотребление привилегиями.

5.3. В перечень инцидентов КБ Стороны включают инциденты, несущие риски потери конфиденциальности,

целостности, доступности данных, указанных в п. 3.1 Соглашения, в том числе:

5.3.1. фишинговая атака от имени Стороны;

5.3.2. эксплуатация выявленной уязвимости на ресурсе, принадлежащем Стороне;

5.3.3. эксплуатация выявленной уязвимости в ПО, предоставляемом/эксплуатируемом Стороной;

5.3.4. заражение ВПО;

5.3.5. НСД к АС / ИР;

5.3.6. DDOS-атака на Информационные ресурсы Стороны.

5.4. В целях оперативного взаимодействия Стороны указывают в Договоре сотрудников, ответственных за обмен информацией о значимых инцидентах (подозрениях на инциденты) КБ.

5.5. В случае устранения значимого инцидента КБ Пользователя обязана не позднее 24 часов после устранения инцидента уведомить ООО «АБТ» о мерах, предпринятых для управления инцидентом.

5.6. 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.

5.7. В рамках обмена информацией об инцидентах КБ Стороны не обмениваются информацией, содержащей банковскую и государственную тайну, тайну связи, персональные данные и иную информацию ограниченного доступа.

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

6. ПЕРСОНАЛЬНЫЕ ДАННЫЕ

6.1. Если по условиям договора, заключаемого между ООО «АБТ» и Пользователем, осуществляется обработка персональных данных, условия обработки и защиты таких данных должны определяться в соответствии с условиями такого договора или отдельного соглашения, посвященного обработке и защите персональных данных в рамках этого договора.

6.2. В случае, если по условиям договора, заключаемого между ООО «АБТ» и Пользователем, одна из Сторон осуществляет обработку персональных данных по поручению другой Стороны, в содержание соответствующего договора должно быть включено поручение на обработку персональных данных, либо Стороны должны заключить отдельный договор поручения обработки персональных данных

6.3. Стороны принимают на себя обязательства обеспечить конфиденциальность и безопасность персональных данных, ставших известными Сторонам в ходе исполнения договоров, указанных в п. 3.1 настоящего Соглашения. Меры, принимаемые для обеспечения безопасности персональных данных и защиты прав субъектов персональных данных, должны соответствовать требованиям законодательства Российской Федерации.

6.4. При обработке персональных данных стороны обязуются принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных в соответствии с требованиями к защите обрабатываемых персональных данных, установленными статьей 19 Федерального закона № 152-ФЗ «О персональных данных» от 27.07.2006 г.

7. УВЕДОМЛЕНИЯ

7.1. Все уведомления, извещения и сообщения в связи с выполнением Соглашения, за исключением сообщений об инцидентах (раздел 5 Соглашения), должны быть оформлены в письменном виде на русском языке и могут быть направлены с помощью электронной почты, заказной или курьерской почтой, с подтверждением факта их получения, по адресу, указанному в Договоре для соответствующей Стороны, либо по иному адресу, о котором любая из Сторон может уведомить другую Сторону. В случае изменения адреса/реквизитов Пользователя, Пользователь обязан направить уведомление с актуальными данными на электронный адрес, указанный ниже, в течение 3 (трех) рабочих дней с момента изменения адреса/реквизита Пользователя.

8. **ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

8.1. Срок действия настоящего Соглашения составляет 5[1] лет с даты его подписания Сторонами. Если в течение месяца до окончания срока действия Соглашения ни одна из сторон не заявила возражение о продлении срока его действия, оно автоматически продлевается на тот же срок на тех же условиях. Срок действия может автоматически продлеваться неограниченное количество раз. Прекращение Соглашения не освобождает Сторону от ответственности за нарушение его условий, имевшее место в период действия Соглашения.

8.2. ООО «АБТ» вправе пересмотреть условия Соглашения по своей инициативе в следующих случаях:

8.2.1. нарушение Пользователем условий, указанных в разделе 3 Соглашения;

8.2.2. наличие у ООО «АБТ» необходимости сохранить надлежащий уровень контроля и управления в отношении риска нарушения КБ Пользователем;

8.2.3. наличие у Правообладателя необходимости принять соответствующие меры для выполнения своих обязательств перед клиентами и контрагентами, а также перед Банком России и уполномоченными государственными органами.

8.3. Стороны несут ответственность в соответствии с законодательством Российской Федерации. В случае нарушения Стороной принятых на себя обязательств по Соглашению, Сторона обязуется возместить другой Стороне убытки (реальный ущерб), причиненные таким нарушением. Убытки возмещаются в соответствии с законодательством Российской Федерации. Возмещение производится не позднее 10 (десяти) рабочих дней со дня получения соответствующего требования от соответствующей Стороны.

8.4. Внесение изменений в Соглашение возможно только путем его перезаключения.

Ни одна из Сторон не может передавать или иным образом уступать, полностью или частично, свои права и обязанности по данному Соглашению без предварительного письменного согласия на это другой Стороны.