Правила оказания услуги
«Аттестация системы защиты информации»,
утвержденные приказом генерального директора
ООО «Белорусские облачные технологии» № 282-ОД от 11.08.2023 (в редакции приказа от 15.08.2025 № 381-ОД)

1. Общие положения

1.1. Настоящие правила оказания услуги «Аттестация системы защиты информации» (далее – Услуга) устанавливают общие условия оказания Оператором Услуги Клиенту, определяют критерии и методы для оценки качества предоставления Услуги, а также порядок взаимодействия Оператора и Клиента и оформления необходимой документации.

1.2. Правила оказания Услуги (далее – Правила) являются неотъемлемой частью Договора на оказание Услуги между Оператором и Клиентом (далее – Договор). Оператор вправе в одностороннем порядке изменять настоящие Правила. Клиент уведомляется об изменении Правил путем публикации на официальном сайте Оператора becloud.by. Подписывая Договор, Клиент принимает обязательность для себя исполнения положений Правил и выражает свое согласие на то, что Правила могут быть изменены Оператором в одностороннем порядке.

2. Термины и определения

2.1. В Правилах и Договоре на оказание Услуги используются следующие термины и определения:

Информационная система (ИС)	информационная система Клиента, предназначенная для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам;
Система защиты информации (СЗИ)	совокупность мер по защите информации, реализованных в информационной системе;
Средства защиты информации (СрЗИ)	совокупность специализированных программно-аппаратных средств защиты информации, применяемых для защиты ИС Клиента, в том числе из состава СЗИ Республиканской платформы;
Анкета	форма сбора данных, предназначенная для получения необходимых сведений от Клиента для целей оказания Услуги;
Аттестация системы защиты информации (Аттестация)	комплекс организационно-технических мероприятий, в результате которых документально подтверждается соответствие

	системы защиты информации требованиям законодательства об информации, информатизации и защите информации;
Аттестат соответствия системы защиты информации информационной системы требованиям по защите информации (далее – Аттестат соответствия)	документ установленной формы, подтверждающий соответствие системы защиты информации требованиям законодательства об информации, информатизации и защите информации;
Веб-ресурс	веб-приложение Клиента, в том числе и его мобильные приложения, располагающееся в сети Интернет и имеющее следующие параметры (но не ограничиваясь): доменное имя, IP-адрес, тип сетевого протокола, тип клиентского сервиса;
Домен (Доменное имя)	символьное (буквенно-цифровое) обозначение, сформированное в соответствии с международными правилами адресации сети Интернет, предназначенное для поименованного обращения к интернет-ресурсу и связанное при его делегировании с определенным сетевым адресом;
Тестирование на проникновение (Пентест)	комплекс мероприятий для получения объективной оценки защищенности информационной системы организации, выявления уязвимостей с целью повышения уровня защищенности ее активов;
Несанкционированный доступ к информации (НСД)	доступ к информации, осуществляемый с нарушением установленных прав или правил разграничения доступа;
Несанкционированное воздействие на информацию (НСВ)	несанкционированное воздействие на информацию – изменение или уничтожение информации, осуществляемое с нарушением установленных прав или правил;
Исполнитель	организация, обладающая необходимыми компетенциями и лицензией, привлекаемая Оператором для выполнения согласованного объема работ в рамках Услуги на основании соответствующего соглашения;

Поддомен (Субдомен)	домен, который является частью основного домена более высокого уровня;
Политика информационной безопасности	общие намерения по обеспечению конфиденциальности, целостности, подлинности, доступности и сохранности информации, документально закрепленные собственником (владельцем) информационной системы;
Метод «серого ящика»	метод проведения работ по тестированию на проникновение в веб-ресурсы Клиента при наличии необходимых прав доступа;
Метод «черного ящика»	метод проведения работ по тестированию на проникновение в веб-ресурсы Клиента при отсутствии каких-либо прав доступа;
Публичный IP-адрес (IP-адрес)	уникальный идентификатор (адрес) элемента веб-ресурса Клиента (либо мобильного приложения) по средствам которого он доступен в сети интернет;
Рабочее место администратора ИС	выделенное автоматизированное рабочее место в организации Клиента для администрирования ИС, соответствующее требованиям, описанным в ТЗ на СЗИ (организация антивирусной защиты, криптографическая защита канала связи с ИС и т.д.), разработанном в рамках оказания Услуги;
Социальная инженерия	метод получения необходимого доступа к конфиденциальной информации Клиента, основанный на особенностях психологии людей;
Применимые правила	правила оказания Услуг Оператором, доступные в сети Интернет на Официальном сайте Оператора, содержащие в себе условия доступа и использование Услуг, изложенные в следующих документах: Правила оказания услуг РЦОД и услуг республиканской платформы, в том числе с использованием технологий облачных вычислений; Правила взаимодействия со Службой поддержки пользователей;
URL	универсальный указатель местоположения веб-ресурсов Клиента в сети Интернет.

2.2. В случае, если в настоящих Правилах и Договоре используются термины, определения которым не даны в разделе «Термины и определения» настоящих Правил, применению подлежат определения таких терминов, данные в Применимых правилах.

3. Описание Услуги

3.1. Услуга является услугой республиканской платформы, относящейся к категории «инфраструктурные услуги» («консультирование, обследование, размещение, настройка, мониторинг, администрирование, техническая поддержка и обслуживание ПТС, информационных ресурсов (систем)»), при оказании которой Оператор обеспечивает проведение мероприятий в сфере технической и криптографической защиты информации, подлежащей обработке в информационной системе, включающих проектирование, создание и аттестацию системы защиты информации ИС Клиента.

3.2. Услуга оказывается в соответствии с требованиями Положения о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, а также Положения о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено (далее – Положение об аттестации), утвержденных приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» (далее – Приказ).

3.3. В рамках Услуги, в зависимости от выбранного тарифа, Оператор обеспечивает:

3.3.1. разработку документации, необходимой для достижения результата оказания Услуги, в следующем объеме[1]:

1) Проект Акта классификации обрабатываемой информации;
2) Проект Акта по отнесению информационной системы к классу типовых информационных систем;
3) Техническое задание на создание системы защиты информации;
4) Общая схема системы защиты информации;
5) Проекты локальных правовых актов и других организационно-распорядительных документов по вопросам применения системы защиты информации[2]:
   – Политика информационной безопасности (корректировка при необходимости);
   – Политика управления учетными записями;
   – Политика физического доступа в здание и помещения;
   – Политика использования паролей;

[1] Все документы разрабатываются в 2 (двух) экземплярах и утверждаются Клиентом. Один утвержденный экземпляр Клиент возвращает в адрес Общества.

[2] Перечень политик согласовывается с Клиентом с учетом действующей политики информационной безопасности Клиента и описанных в ней положений. В рамках Услуги разработке подлежат только политики, отсутствующие у Клиента и необходимые для аттестации информационной системы.

– Политика контроля и мониторинга функционирования ИС;
– Политика резервирования, хранения и уничтожения данных;
– Политика реагирования на инциденты информационной безопасности;
– Политика антивирусной защиты;
– Политика выявления уязвимостей;
– Политика использования съемных носителей;
– Политика использования электронной почты;
– Политика обновления средств защиты информации;
– Политика управления криптографическими ключами;

6) Программа и методика аттестации;
7) Технический отчет;
8) Протокол испытаний системы защиты информации информационной системы;

3.3.2. реализацию мероприятий:

– проверка правильности отнесения информационной системы к классу типовых ИС;

– анализ документации на ИС Клиента и компоненты ее защиты на предмет ее соответствия требованиям законодательства об информации, информатизации и защите информации;

– установление соответствия фактического состава активов ИС структурной и логической схемам ИС;

– ознакомление с документацией о распределении функций персонала Клиента по организации и обеспечению защиты информации;

– проверку достаточности реализованных в системе защиты информации мер по защите информации, в том числе:

– анализ локальных правовых актов и других организационно-распорядительных документов по вопросам применения системы защиты информации на предмет их соответствия требованиям законодательства об информации, информатизации и защите информации;

– проведение испытаний системы защиты информации на предмет выполнения установленных законодательством требований по защите информации;

– внешнюю и внутреннюю проверку отсутствия либо невозможности использования нарушителем свойств активов ИС, средств защиты информации, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих активов ИС, средств защиты информации[1];

– оценку эффективности защищенности ИС классов «3-бг» и (или) «3-дсп» (тестирование на проникновение);

---

[1] В стоимость Услуги входит **предварительное сканирование** информационных активов (внешнее и внутреннее), **повторное сканирование осуществляется** после исправления Клиентом выявленных недостатков и уязвимостей. В случае, если повторное сканирование выявило недостатки и уязвимости, Клиент **обязан оформить дополнительный Заказ** на очередное сканирование на основании действующих тарифов Оператора.

– оформление технического отчета и протокола испытаний;

– оформление аттестата соответствия в случае успешного завершения аттестационных испытаний ИС Клиента.

3.3.3. проведение Пентеста – **опционально** (при указании Клиентом в Заказе), **обязательно** (для ИС классов «3-бг» и (или) «3-дсп») результатом которого является отчет, содержащий:

1) перечень выявленных уязвимостей с оценкой степени их критичности;

2) результаты проведенных атак и эксплуатации уязвимостей с демонстрацией примеров их реализации;

3) перечень рекомендаций по устранению обнаруженных уязвимостей;

4) информацию о результате сканирования веб-ресурсов с использованием автоматизированного средства контроля защищенности (сканирование уязвимостей);

5) рекомендации по классификации информации, хранящейся и обрабатываемой в соответствии с законодательством;

6) рекомендации к отнесению содержащей информации к классу типовых информационных систем;

7) рекомендации по определению требований к системе защиты информации, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

3.4. В рамках оказания Услуги Оператор взаимодействует с представителями Клиента – собственника (владельца) ИС, в том числе для согласования положений разрабатываемых документов.

3.5. Для обеспечения качества предоставления Услуги Оператор с уведомлением Клиента может привлекать Исполнителя. В таком случае Оператор отвечает перед Клиентом за действия Исполнителя в рамках проведения данных работ как за свои собственные.

3.6. При подтверждении соответствия системы защиты информации требованиям законодательства об информации, информатизации и защите информации Оператор оформляет и передает Клиенту Аттестат соответствия.

4. Ограничения и соглашения

4.1. Оператор имеет право в одностороннем порядке приостановить оказание Услуги до устранения нарушений в случае неисполнения или ненадлежащего исполнения Клиентом обязательств, указанных в Договоре и Правилах.

4.2. В случае запроса Оператором у Клиента недостающей информации, необходимой для оказания Услуги, сроки оказания Услуги увеличиваются соразмерно времени, необходимому Клиенту для предоставления запрошенной Оператором информации. Время продления сроков выполнения услуги определяется как разница во времени между исходящим запросом Оператора и полученным ответом Клиента.

4.3. Недостающая для надлежащего оказания Оператором Услуги информация и документация, перечисленная в Календарном плане, передаются посредством специализированного файлового ресурса Оператора либо через

Личный кабинет (далее – ЛК), за исключением оригинальных экземпляров Договоров, Актов сдачи-приемки оказанных услуг, утвержденных документов и Аттестата, оригинальные экземпляры которых передаются почтовым отправлением или иным согласованным Сторонами способом.

4.4. После утверждения, разработанного Оператором технического задания на создание системы защиты информации Клиенту запрещается вносить в аттестуемую ИС изменения (изменять ее состав, архитектуру, структуру и логику функционирования, добавлять/изменять состав внешних ИС и сервисов, с которыми взаимодействует аттестуемая ИС). В случае выявления фактов внесения изменений в ИС на любом из этапов работ, предусмотренных в рамках оказания услуги Оператор вправе приостановить оказание Услуги в одностороннем порядке. Клиент может повторно обратиться за оказанием Услуги, при этом Услуга будет оказываться Оператором на основании отдельно заключенного договора.

4.5. После завершения этапа по созданию системы защиты информации ИС Оператор направляет Клиенту Уведомление о готовности к проведению Аттестации или Уведомление о наличии несоответствий критериям Аттестации. Клиент обязуется устранить недостатки, выявленные Оператором (при их наличии) в течение 80 (восьмидесяти) календарных дней со дня получения уведомления. В случае невозможности устранения Клиентом выявленных недостатков в указанный срок Оператор вправе приостановить оказание Услуги в одностороннем порядке.

4.6. В случае, если Клиент устранил недостатки ИС после приостановления оказания Услуги, но в результате обеспечил соответствие рекомендациям Оператора и, при этом, не вносил иные изменения в ИС и проектируемую Оператором СЗИ ИС (обязательное условие), то, по согласованию с Оператором, он может повторно обратиться за оказанием Услуги, начиная с этапа «Аттестация системы защиты информации Информационной системы». При этом Услуга будет оказываться Оператором на основании отдельно заключенного договора.

4.7. В соответствии с Положением об аттестации:

аттестация вновь создаваемой СЗИ осуществляется до ее ввода в эксплуатацию;

срок проведения Аттестации в рамках тарифа «Система» не может превышать 180 (сто восемьдесят) календарных дней при условии согласования и последующего подписания с Оператором актов выполненных работ в рамках календарного плана;

Аттестат соответствия действителен при обеспечении неизменности технологии обработки защищаемой информации и (или) технических мер, реализованных при создании или модернизации системы защиты информации. В случае изменения указанных требований Аттестация должна проводиться повторно;

Аттестат соответствия оформляется сроком на 5 (пять) лет. После окончания срока Аттестация проводится Клиентом заново на основе отдельно заключаемых договоров.

4.8. В случае заказа тарифа «Спринт» ИС Клиента должна соответствовать следующим условиям:

класс аттестуемой ИС должен соответствовать классу типовых информационных систем 3-ин (информационные системы, в которых обрабатываются персональные данные, за исключением специальных персональных данных, и которые подключены к открытым каналам передачи данных);

ИС не должна иметь информационного взаимодействия с внешними информационными системами (отсутствуют информационные потоки либо связи с внешними информационными системами и/или ресурсами);

в ИС применяются СрЗИ из состава СЗИ Республиканской платформы;

подключение к ИС осуществляется только с помощью СрЗИ;

4.9. Срок проведения Аттестации в рамках тарифа «Спринт» не превышает 30 (тридцать) календарных дней при условии выполнения положений ТЗ и предоставления Клиентом всех заполненных шаблонов документов, полученных от Оператора в рамках оказания Услуги.

4.10. Проведение Пентеста осуществляется только в случае размещения веб-ресурсов Клиента на ресурсах Республиканской платформы либо при оценке эффективности защищенности ИС классов «3-бг» и (или) «3-дсп» в рамках оказания Услуги.

4.11. Пентест проводится удаленно (из сети Интернет) в рабочие дни с учетом периода времени, указанного Клиентом в Заказе. Перед выполнением Пентеста Оператор дополнительно согласует время его проведения с Клиентом.

4.12. При проведении Пентеста:

возможны прерывания в функционировании веб-ресурсов или ИС Клиента. При возникновении такого случая Оператор информирует о нем ответственного сотрудника со стороны Клиента, указанного в Заказе и оказывает консультативную помощь;

использование социальной инженерии допускается только как метод оценки осведомленности сотрудников в вопросах информационной безопасности.

4.13. **Оператор обязуется:**

4.13.1. оказать Клиенту Услугу надлежащим образом, в объеме и в сроки, предусмотренные Договором;

4.13.2. предоставлять Клиенту консультации в рамках использования Услуги со стороны уполномоченных лиц Оператора;

4.13.3. вести учет оказания и оплаты Клиентом Услуги в соответствии с Заказами;

4.13.4. своевременно информировать Клиента о возникших ситуациях, затрудняющих получение результатов выполнения Услуги;

4.14. **Клиент обязуется:**

4.14.1. обеспечить своевременное предоставление запрошенных Оператором Исходные данные (в случае непредоставления / неполного предоставления Исходных данных Оператор оставляет за собой право не

приступать к оказанию Услуги либо отказаться от исполнения договора на оказание Услуги);

4.14.2. в течение 5 (пяти) рабочих дней обеспечивать согласование проектов документов, предоставляемых Оператором; при этом сроки исполнения обязательств Оператора увеличиваются соразмерно сроку превышения Клиентом сроков согласования;

4.14.3. в течение 5 (пяти) рабочих дней с даты передачи рассмотреть согласованные ранее документы, подписать и утвердить их в 2-х экземплярах. Один подписанный и утвержденный экземпляр направить в адрес Оператора. В случае наличия замечаний, Клиент направляет в адрес Оператора мотивированный отказ от подписания документов. Оператор устраняет недостатки в согласованные с Заказчиком сроки. В случае отсутствия мотивированного отказа в течение 5 (пяти) рабочих дней Услуга (этап) считается оказанной в полном объёме и подлежит оплате.

4.14.4. оказывать разумное содействие Оператору и Исполнителю при оказании Услуги, включая предоставление дополнительных документов и (или) информации, необходимых для своевременного и качественного оказания Услуги;

4.14.5. предоставить тестовые (временные) учетные данные для получения доступа к системам/сервисам веб-ресурсов (в случае проведения Пентеста методом «серого ящика»); после проведения Пентеста тестовые учетные данные подлежат удалению Клиентом;

4.14.6. перед началом Пентеста выполнить резервное копирование веб-ресурсов в соответствии с принятой у Клиента политикой резервного копирования. В случае их недоступности в результате или во время проведения Пентеста выполнить восстановление работоспособности своими силами и за свой счет;

4.14.7. в случае возникновения ситуаций, препятствующих выполнению Пентеста, в том числе вызванных некорректным функционированием веб-ресурсов/ИС (нарушение доступности, блокирование IP-адресов или учетных записей и т. п.), самостоятельно обеспечивать восстановление функционирования веб-ресурсов/ИС в штатном режиме. При возникновении подобных ситуаций срок проведения Пентеста продлевается на срок, требуемый Клиенту на разрешение описанных ситуаций;

4.14.8. обеспечивать урегулирование ситуаций, связанных с возможными претензиями к Оператору со стороны третьих лиц, полученных в результате проведения Пентеста;

4.14.9. обеспечивать устранение недостатков, выявленных Оператором в процессе оказания Услуги, в сроки, установленные Договором и иными документами;

4.14.10. руководствоваться Применимыми правилами в рамках использования Услуги;

4.14.11. обеспечивать знание и соблюдение требований Применимых правил (Клиент гарантирует, что уровень его знаний будет достаточным для использования Услуги);

4.14.12. обеспечивать сохранность и конфиденциальность информации по исполнению Договора на оказание Услуги, полученной от Оператора;

4.14.13. направить в Оперативно-аналитический центр при Президенте Республики Беларусь копию аттестата соответствия системы защиты информации ИС требованиям по защите информации, технического отчета и протокола испытаний посредством получения электронных услуг общегосударственной автоматизированной информационной системы с использованием личных электронных кабинетов или системы межведомственного электронного документооборота государственных органов Республики Беларусь в течение 10 (десяти) календарных дней со дня оформления (получения) Аттестата соответствия (в соответствии с подпунктом 4.3 пункта 4 Положения о порядке представления в Оперативно-аналитический центр при Президенте Республики Беларусь сведений о событиях информационной безопасности, состоянии технической и криптографической защиты информации, утвержденного приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449».

4.15. **Оператор не несет ответственность:**

4.15.1. за доступность и работоспособность ИС и веб-ресурсов Клиента при оказании Услуги;

4.15.2. в случае невозможности использования Услуги и выполнения согласованных действий по причинам, не зависящим от Оператора;

4.15.3. за убытки, которые может понести Клиент вследствие использования Услуги и ее результатов.

5. Стоимость услуги

5.1. Стоимость Услуги формируется на этапе согласования Заказа на основании действующих тарифов Оператора.

5.2. При расчете стоимости Услуги учитывается факт указания в Заказе на необходимость проведения повторного сканирования, Пентеста, а также (в случае проведения Пентеста) количество уникальных URL в составе веб-ресурса/ИС Клиента.

5.3. В случае заказа Клиентом Пентеста:

1) используются следующие принципы расчета количества тарифицируемых URL:

домен эквивалентен IP-адресу или мобильному приложению;

домены третьего и последующего уровней расцениваются, как дополнительный URL;

2) количество доменов в одном Заказе не должно превышать 10 (десять);

3) в случае необходимости проверки более 10 (десяти) доменов Клиент имеет возможность оформить дополнительный Заказ. Стоимость рассчитывается на основании действующих тарифов Оператора.

5.4. Оплата за оказание Услуги осуществляется в соответствии с Договором.

6. Порядок оказания услуги

6.1. Запрос на оказание Услуги может быть оформлен посредством заполнения формы обратной связи (выбор действия «Связаться с нами» в разделе «Контакты»-«Контактная информация» на Сайте Оператора) с указанием данных о Клиенте согласно форме Заказа, а также полного наименования организации Клиента и реквизитов для оформления Договора либо с помощью функций ЛК.

6.2. Обработка запросов в рамках оказания Услуги производится в Стандартное рабочее время. В случае поступления запроса в нерабочее время, обработка осуществляется в течение следующего рабочего дня.

6.3. В течение рабочего дня, следующего за днем получения запроса на оказание Услуги, Оператор направляет Клиенту соглашение о неразглашении и проект Договора.

6.4. Определение параметров Услуги осуществляется путем согласования Заказа в соответствии с формами, утвержденными в рамках настоящих Правил.

6.5. Перед оказанием Услуги между Оператором, Исполнителем и Клиентом заключается соглашение о конфиденциальности, затрагивающее все возможные аспекты предоставления Услуги, а также обмен технической и коммерческой информацией.

6.6. Для обеспечения возможности оказания Услуги в зависимости от выбранного тарифа Клиент предоставляет Оператору набор исходных данных (далее – Исходные данные) в следующем объеме:

заполненная Анкета;

приказ о создании аттестационной комиссии (в аттестационную комиссию должен быть включен представитель юридической службы Клиента);

акт отнесения информационной системы к классу типовых информационных систем;

наименование информационной системы, ее назначение, область применения;

политику информационной безопасности;

структурную и логическую схему информационной системы;

документ, подтверждающий наличие у собственника (владельца) информационной системы подразделения технической защиты информации или иного подразделения (должностного лица), выполняющего функции по технической и (или) криптографической защите информации;

описание информационной системы, включающее общую функциональную схему, физические и логические границы, информационные потоки и протоколы обмена защищаемой информацией, а также места размещения элементов системы (аппаратных и программных) и средств защиты информации;

копии сертификатов соответствия либо экспертных заключений на средства защиты информации;

документы, свидетельствующие о наличии действующей технической поддержки (сервисные контракты) на применяемые средства защиты информации;

основные характеристики инженерно-физических средств защиты, технических средств и систем охраны информационной системы, в том числе помещений, в которых обрабатывается защищаемая информация и хранятся носители информации.

6.7. Оператор приступает к оказанию Услуги после согласования проведения работ с Оперативно-аналитическим центром при Президенте Республики Беларусь.

6.8. В день передачи Клиентом всех документов в объёме, описанном в п.6.6, а также при условии выполнения требований п.6.7, Оператор направляет Клиенту Уведомление о начале Проектирования системы защиты информации Информационной системы.

6.9. Обмен документами производится посредством специализированного файлового ресурса Оператора либо с использованием функций ЛК.

6.10. Проведение испытаний СЗИ на предмет выполнения требований по защите информации, установленных законодательством, может быть выполнено с использованием средств видеоконференцсвязи или иным способом по согласованию с Клиентом.

6.11. Запросы на изменение параметров Услуги направляются через ЛК. Изменение параметров Услуги оформляется подписанием нового Заказа.

6.12. Уполномоченное лицо Клиента может сообщить свои претензии о несвоевременном или некачественном выполнении запроса или предложения по улучшению Услуги.

6.13. Все претензии регистрируются и передаются ответственному лицу Оператора, которое контролирует процесс удовлетворения претензии и получает от заявителя подтверждение факта решения в устной или письменной форме.

6.14. Все претензии должны быть рассмотрены в течение срока, определенного внутренними регламентами Оператора.

ФОРМЫ ДОКУМЕНТОВ

Форма

Заказ № ____ от «___»_____20__ г.

к Договору №____от «___» _____202_ г.

оказания Услуги «Аттестация системы защиты информации»

Клиент:

Тип заказа: (новая Услуга, изменение Услуги)

Дата начала оказания Услуг:

Срок оказания Услуги: с __.__.202__ (при условии предоставления исходных данных) по __.__.202__.

Объем Услуг, запрашиваемых Клиентом:

№	Наименование Тарифа	Значение выбора
1.	Тариф <*название тарифа*>	☐
1.1		
2.		
3.	Дополнительные работы	
3.1		
	Сумма НДС, 20%, руб.*	
	Стоимость услуги: сумма без НДС _____, сумма НДС* _____, всего с НДС* _____	

* - без НДС в соответствии с подп.2.2 пункта 2 Указа Президента Республики Беларусь от 23.01.2014 № 46.

Оператор:

ООО «Белорусские облачные технологии»
220004, Республика Беларусь,
г. Минск, ул. К. Цеткин, 24, пом.602,
УНП 191772685
р/с BY14BAPB30127209600100000000 (933)
в ОАО «Белагропромбанк», BAPBBY2X
г. Минск, пр.Жукова, д.3

_____/ /

М.П.

Клиент:

_____/ /

М.П.

Форма

Заказ №_____ от «_____»_____20__ г.

к Договору № __ от «___» _____ 20__ г.

оказания услуги республиканской платформы «Аттестация системы защиты информации»

(ТЕХНИЧЕСКАЯ ЧАСТЬ)

Информация для определения объема работ при тестировании веб-ресурсов/ИС Клиента на проникновение (Пентест):

1	Перечень проверяемых доменов или IP-адресов включающие поддомены и URL	Доменное имя (IP-адрес)	URL (поддомены)
		Пример: *1) example.com* *2) 12.13.14.1*	*Пример:* *1) https://example.com/site* *2) one.example.com*
2	Список тестируемых мобильных приложений с указанием его названия либо используемого им IP-адреса и платформы (iOS, Android)	*Пример:* *1) application1 (Android, iOS)* *2) application2 (iOS)* *3) 12.13.14.1*	
3	Управление ИТ и ИБ централизовано?	*Пример: Да*	
4	Укажите цели анализа защищенности		
4.1	Выявление всех возможных уязвимостей вне зависимости от степени их критичности	*Пример: Да*	
4.2	Выявление наиболее критических уязвимостей и способов их эксплуатации (тест на проникновение)	*Пример: Да*	
5	Укажите состав работ по анализу защищенности		
5.1	Проведение внешнего анализа защищенности (из сети Интернет)	*Пример: Да*	
5.2	Проведение внутреннего анализа защищенности (из сети организации)	*Пример: Да*	
5.3	Тестирование веб-ресурсов[1]	*Пример: Да*	
5.4	Тестирование мобильных приложений[2]	*Пример: Нет*	
6	Укажите методы анализа защищенности которые необходимо использовались		
6.1	Анализ защищенности методом «черного ящика» (без предоставления реквизитов доступа к системам/сервисам)	*Пример: Не использовать*	
6.2	Анализ защищенности методом «серого ящика» (с предоставлением санкционированного доступа к системам/сервисам)	*Пример: Использовать*	
6.3	Методы социальной инженерии	*Пример: Использовать/Не использовать*	
7	Желаемое время и дата начала работ	*Пример: Дата 01.01.2024, Время начала 9:00*	
8	Желаемое время и дата окончания работ	*Пример: Дата 01.01.2024, Время окончания 15:00*	

[1] Тестирование веб-ресурсов проводится в соответствии с OWASP Testing Guide с фокусом на уязвимости списка OWASP Top 10 Application Security Risks;

[2] Тестирование мобильных приложений производится в соответствии с Mobile Security Testing Guide (MSTG) с фокусом на уязвимости из списка OWASP Mobile Top 10.

9	Адрес электронной почты для получения отчета по результатам проведения работ в рамках оказываемой услуги	*Пример: security@email.com*
10	Сотрудник Клиента ответственный за информационную безопасность и доступность ИС при проведении тестирования (ФИО, контактный телефон, адрес электронной почты)	

Форма

Акт сдачи-приемки оказанных услуг №_____

по услуге республиканской платформы «Аттестация системы защиты информации»
к Договору №_____ от «___» _____ 202_ г.
оказания услуги республиканской платформы «Аттестация системы защиты информации»

г. Минск «____» _____20__ года

В соответствии с Договором № __ оказания услуги республиканской платформы «Аттестация системы защиты информации» от «___» _____ 202_ г., настоящим Актом сдачи-приемки оказанных Услуг Оператор и Клиент удостоверяют, что:

1. Оператор оказал Клиенту Услуги республиканской платформы «Аттестация системы защиты информации» в соответствии с таблицей:

№ п/п	Заказ (№, дата)	Период оказания Услуги	Стоимость без НДС, бел. руб.
1.			
2.			
Итого стоимость, бел.руб.			
Сумма НДС по ставке 20%*, бел.руб.*			
Всего с НДС, бел.руб.*			

Итого оказано услуг на сумму: _____ (_____)
с учетом НДС по ставке 20%*
в том числе НДС по ставке 20%* составляет: _____ (_____).

* - без НДС в соответствии с п.2.2 Указа Президента Республики Беларусь от 23.01.2014 № 46 в редакции Указа Президента Республики Беларусь от 16.12.2019 № 461

2. Услуги оказаны в полном объеме. Клиент не имеет претензий к Оператору по качеству оказанных услуг.

3. Настоящий Акт составлен на русском языке в двух экземплярах, каждый из которых имеет одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

4. Подписание Акта Сторонами свидетельствует о сдаче-приемке оказанных услуг и является основанием для проведения оплаты.

Подписи сторон:

Оператор:

Общество с ограниченной ответственностью «Белорусские облачные технологии»
р/с BY14BAPB30127209600100000000
в ОАО «Белагропромбанк»,
БИК BAPBBY2X
Адрес: 220004, Республика Беларусь,
г. Минск, ул. К. Цеткин, 24, пом.602,
тел.: +375 (17) 287-11-11
e-mail: sales@becloud.by
e-mail: finance@becloud.by
УНП 191772685

Клиент: