Приложение №8

к Тарифам на оказываемые услуги

ГУП «Центр кибербезопасности»

**Регламент оказания услуги**

**«Разработка Политики информационной безопасности»**

## 1. Описание (паспорт) услуги

1.1. Наименование услуги:

разработка Политики информационной безопасности.

1.2. Результат услуги:

предоставление заявителю проекта разработанной Политики информационной безопасности для последующего его согласования и утверждения в установленном порядке.

1.3. Организация, оказывающий услугу:

ГУП «Центр кибербезопасности». Форму заявки и договора можно получить на официальном сайте ГУП «Центр кибербезопасности» https://csec.uz, а также по адресу: г. Ташкент, Мирабадский район улица Тараса Шевченко, дом 20.

1.4. Правовые основания:

постановление Президента Республики Узбекистан от 21 июня
2020 года № ПП-4751 «О мерах по совершенствованию системы обеспечения кибербезопасности в Республике Узбекистан».

1.5. Срок подачи запроса:

 по мере необходимости.

1.6. Срок исполнения:

 срок исполнения устанавливается согласно договору.

1.7. Срок выдачи подтверждения:

 в течении 3-х рабочих дней с момента получения заявки на оказание услуги, соответствующим уведомлением.

**2. Информирование получателей услуги**

2.1. Состав и объем информации:

Любому обратившемуся за услугой лицу гарантируется предоставление следующей информации:

- местонахождение ГУП «Центр кибербезопасности», оказывающего услугу, график работы, процедура приема посетителей (предварительная запись по телефону, прием в рабочее время и т.п.);

- способ получения или предоставление формы заявки и договора;

- порядок оплаты;

- процедура оказания услуги;

- срок исполнения оказываемой услуги;

- наличие регламента услуги и способ ознакомления с ним.

2.2. Подробная информация:

 Стандартную информацию о предоставляемых услугах и обслуживанию можно получить:

- по адресу: 100115, г. Ташкент, Мирабадский район улица Тараса Шевченко, дом 20.

- по телефону: (+99871) 203-00-26;

- через официальный сайт ГУП «Центр кибербезопасности» https://csec.uz.

2.3. Информирование по запросу:

 Лично: заявитель может обращаться с 9:00 до 18:00 по любым вопросам по предоставлению услуги (реквизитах оплаты, перечне необходимых документов и т.д.);

 По телефону: с 9:00 до 18:00 доступно устное консультирование по любым вопросам в части предоставления услуги.

2.4. Используемые формы документов:

- официальное письмо-заявление в адрес ГУП «Центр кибербезопасности» на оказание услуги;

- договор между сторонами об оказании услуги.

## 3. Обслуживание

3.1. Время работы:

 Время работы с 9.00 до 18.00.

 Обед с 13.00 до 14.00.

 Выходные дни: суббота, воскресенье.

## 4. Процедура оказания услуги

4.1. Предоставление информации для оказания услуги:

Для оказания услуги заказчик услуги должен предоставить информацию ГУП «Центр кибербезопасности», необходимую для разработки Политики информационной безопасности согласно разработанному вопроснику.

Сбор информации производится на месте размещения заказчика путем анкетирования его специалистов, владеющих данной информацией, и осмотра имеющихся у заявителя объектов и средств защиты. При необходимости производится выезд на иные объекты заказчика.

Заказчик также должен предоставить имеющиеся у него внутренние нормативные документы в области обеспечения информационной безопасности и матрицы доступа к информационным ресурсам при условии их наличия.

4.2. Платность услуги:

Для органов государственного и хозяйственного управления, государственной власти на местах и иных юридических лиц услуга оказывается на платной основе.

4.3. Этапы оказания услуги:

Услуга оказывается на основании заявки согласно приложению №1 к настоящему Регламенту. На основании заявки определяется и согласовывается сторонами объем, стоимость и сроки оказания услуги и оформляется договор согласно приложению №3 к настоящему Регламенту.

После заключения договора услуга оказывается согласно схеме, приведенной в приложении №2 к настоящему Регламенту, с выполнением следующих этапов:

- 1-этап- производится сбор информации, необходимой для разработки Политики информационной безопасности. При необходимости ГУП «Центр кибербезопасности» направляет заявителю запрос на предоставление требуемой конфиденциальной информации.

- 2-этап-осуществляется разработка Политики информационной безопасности в соответствии с принятым Методическим пособием по разработке политики информационной безопасности на территории Республики Узбекистан» и иными нормативными документами в области обеспечения информационной и кибербезопасности.

- 3-этап-проект разработанной Политики информационной безопасности направляется на рассмотрение заказчику. По результатам рассмотрения сторонами устраняются имеющиеся недостатки, замечания и неточности.

- 4-этап-в случае отсутствия замечаний со стороны заявителя ему вносится окончательный проект разработанной Политики информационной безопасности вместе с актом приема - передачи результатов работ.

Оказание услуги завершается подписанием акта приема - передачи результатов работ заказчиком.

4.4. Взаимодействие сторон при оказании услуги:

 Для эффективного взаимодействия заказчик должен выделить своего координирующего специалиста, с которым ГУП «Центр кибербезопасности» будет взаимодействовать при оказании услуги и информировать его о ходе выполнения работ.

4.5. Основания отказа:

Основанием отказа в оказании услуги является отказ заказчика в предоставлении информации, требуемой для разработки Политики информационной безопасности, и от иных обязательств, определенных в договоре.

**5. Обеспечение качества**

5.1. Обжалование некачественной услуги:

 Заявитель может обратиться с официальным письмом на имя руководителя ГУП «Центр кибербезопасности» с указанием причин несогласия с результатами полученной услуги или обжаловать в установленном законодательством порядке.

Приложение №1

к Регламенту на оказание услуги «Разработка Политики информационной безопасности»

*На фирменном бланке учреждения*

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_№ \_\_\_\_\_\_\_\_\_\_\_\_\_  | **ГУП «Центр кибербезопасности»**  |

**ЗАЯВЛЕНИЕ**

**на разработку Политики информационной безопасности**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
*(наименование организации)*

просит разработать Политику информационной безопасности в соответствии с требованиями нормативных документов.

1. Адрес: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Банковские реквизиты:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Своевременная оплата за оказываемую услугу гарантируется.

Руководитель организации \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (должность) личная подпись

Приложение №2

к Регламенту на оказание услуги «Разработка Политики информационной безопасности»

**Схема оказания услуги**

**по разработке Политики информационной безопасности**

**Сокращения:**

Центр - ГУП «Центр кибербезопасности»;

Заявитель - организация.

**Этапы**

**Участники**

**Сроки**

**Мероприятия**

Заявитель

По факту обращения

Подача заявки на оказание услуги

Центр, заявитель

5 рабочих

дней

Подготовка и подписание договора

Заявитель

10 банковских дней

Перечисление предоплаты по договору

**1-этап**

Центр

В течении 4 рабочих дней

Сбор информации для разработки Политики информационной безопасности

**2-этап**

Центр

В течении 20 рабочих дней

Разработка проекта Политики информационной безопасности

**3-этап**

Центр, заявитель

5 рабочих дней

Внесение Центром проекта Политики заявителю. Рассмотрение проекта Политики заявителем. Устранение Центром недостатков и замечаний заявителя

**4-этап**

Центр

3 рабочих дня

Внесение окончательной версии проекта Политики и акта сдачи приема работ заявителю

Заявитель

2 рабочих дня

Подписание акта сдачи-приема работ

Приложение №3

к Регламенту на оказание услуги «Разработка Политики информационной безопасности»

**Расчет тарифа услуг по разработке политики информационной безопасности**

|  |  |  |
| --- | --- | --- |
| **№****п/п** | **Состав работ** | **Трудоемкость работ сх. № 1** |
| **Кол-во спец-ов** | **Кол-во****часов** | **Общее кол-во ч/часов** |
| **1** | **2** | **3** | **4** | **5** |
| **1** | Проведение предварительного обследования состояния информационной безопасности | --- | --- | --- |
| 1.1 | Проведение инвентаризации, определение объектов защиты (информационные ресурсы, сети, ресурсы, технические средства обработки информации, помещения, где установлены и эксплуатируются эти средства, и предназначенные для ведения переговоров, в том числе конфиденциального характера) | 2 | 2 | 4 |
| 1.2 | Идентификация угроз информационной безопасности | 2 | 1 | 2 |
| 1.3 | Оценка принятых организационно-правовых мер защиты и используемых средств защиты информации | 2 | 1 | 2 |
| 1.4. | Определение рисков информационной безопасности | 1 | 2 | 2 |
| **2** | Разработка политики информационной безопасности | --- | --- | --- |
| 2.1 | Указание целей и задач, объектов защиты, рисков и модели угроз информационной безопасности | 1 | 2 | 2 |
| 2.2 | Определение и указание мер информационной безопасности | 1 | 4 | 4 |
| 2.3. | Разработка документов, входящих в состав политики информационной безопасности (положения, инструкции, правила, перечней, порядков и планов) | 2 | 4 | 8 |
| 2.4. | Классификация информации и информационных ресурсов, разработка матриц доступа | 1 | 2 | 2 |
|  | **И Т О Г О:** | **26,0 ч/часов** |

Для разработки политики информационной безопасности, вовлекаются 2 специалиста, время работы одного специалиста 13 часов, суммарное время оказания услуги 26 часов, общая сумма оказываемых услуг составляет 8 875 694‬ (восемь миллионов девятьсот семьдесят пять тысяч шестьсот девяносто четыре) сум, с учётом НДС.

Сумма, подлежащая к оплате 8 875 694‬ (восемь миллионов девятьсот семьдесят пять тысяч шестьсот девяносто четыре) сум.

Приложение №4

к Регламенту на оказание услуги «Разработка Политики информационной безопасности»

**Договор №\_\_\_\_\_\_\_\_**

**на оказание услуги «Разработка Политики информационной безопасности»**

г. Ташкент «\_\_\_» \_\_\_\_\_\_\_\_20\_\_ года

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемый в дальнейшем «Заказчик», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующей на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с одной стороны, и ГУП «Центр кибербезопасности», именуемый в дальнейшем «Исполнитель», в лице Директора О. Мираева, действующего на основании Устава с другой стороны, совместно именуемые Стороны, заключили настоящий Договор
о нижеследующем.

**1. ПРЕДМЕТ ДОГОВОРА**

**1.1.** По настоящему Договору Заказчик поручает и оплачивает, а Исполнитель принимает на себя обязательство оказать содействие по разработке политики информационной безопасности, именуемую в дальнейшем «Услуга».

Заказчик принимает и оплачивает результаты Услуги.

**1.2.** Политика информационной безопасности должна быть разработана в соответствии с требованиями нормативных документов в области информационной безопасности и Приложением №10 «Методические пособия по разработке политики информационной безопасности на территории Республики Узбекистан» к протоколу Республиканской комиссии по координации реализации Комплексной программы развития Национальной информационно-коммуникационной системы РУз на 2013-2020гг.
от 23.02.2016г. за №7.

**1.3.**По результатам оказания Услуги Исполнитель предоставляет Заказчику разработанную политику информационной безопасности, которая выдаётся Заказчику на руки или путем направления через Государственную фельдъегерскую службу (нарочно).

**1.4.**Срок разработки политики информационной безопасности не должен составлять более \_\_\_ ***(\_\_\_\_\_\_\_\_\_\_)* месяца** со дня поступления Исполнителю предоплаты в порядке, указанном в пункте 2.3. настоящего Договора.

**1.5.**Оказание Услуги считается завершённым с момента направления (вручения) Заказчику разработанной политики информационной безопасности.

**1.6.** Все расходы, связанные с выполнением настоящего Договора
и не согласованные Сторонами как расходы Заказчика, Исполнитель несёт самостоятельно за счёт собственных средств.

**2. СТОИМОСТЬ УСЛУГ И ПОРЯДОК ОПЛАТЫ**

**2.1.** Стоимость оказываемых Услуг по настоящему Договору составляет
**\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ) сум**с учётом НДС.

**2.2.** Вид расчётов - перевод денежных средств на расчётный счет Исполнителя платежными поручениями.

**2.3.** Заказчик в течение **10 *(десяти)*** **банковских дней** с момента подписания настоящего Договора перечисляет на расчётный счет Исполнителя предоплату в размере **30 %** от общей стоимости работ – **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)* сум**с учётом НДС.

**2.4.** По результатам окончания оказываемой Услуги Исполнитель предъявляет Заказчику Акт сдачи-приёмки оказанной Услуги (далее – Акт) и счет-фактуру установленного образца в течение **5 *(пяти)* банковских дней**.

**2.5.**Окончательная оплата в размере **70 %** от общей стоимости Услуг составляет
**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)* сум** с учётом НДС, которая подлежит к оплате в течение **3 *(трех)* банковских дней** с момента подписания Акта.

**3. ОБЯЗАТЕЛЬСТВА СТОРОН**

**3.1.**Заказчик обязуется:

определить ответственное лицо, в обязанности которого входит предоставление от Заказчика исходной информации, необходимой для разработки политики информационной безопасности;

обеспечить беспрепятственный доступ представителей Исполнителя в здание и помещения Заказчика для изучения текущего состояния информационной безопасности, определения перечня имеющихся у Заказчика объектов защиты, оборудования и средств обеспечения информационной безопасности;

предоставлять достоверную информацию касательно имеющегося оборудования в информационной инфраструктуре Заказчика, их доступности и активности в сети;

требовать от Исполнителя оказания Услуги соответствующего качества и в полном объеме;

принять от Исполнителя оказанную Услугу в полном объеме и соответствии с настоящим Договором и оплатить её по стоимости и в порядке, указанном в разделе 2 настоящего Договора.

**3.2.** Исполнитель обязуется:

оказать Заказчику Услугу в сроки, в полном объеме и качественно в соответствии разделом 1 настоящего Договора

в соответствии с требованиями нормативных документов в области информационной безопасности провести анализ имеющейся организационно-распорядительной документации по вопросам информационной безопасности, изучение существующей информационной инфраструктуры Заказчика и оценку состояния обеспечения информационной безопасности;

передать Заказчику разработанную политику информационной безопасности на бумажном носителе в **1 *(одном)*** **экземпляре** и в электронной форме;

выставлять Заказчику счет для оплаты оказанной Услуги и после завершения оказания Услуги предоставить ему Акт в сроки и порядке, предусмотренном в разделе 2 настоящего Договора;

по требованию Заказчика безвозмездно исправить все выявленные недостатки, если в процессе оказания Услуги Исполнитель допустил отступления от условий Договора.

**4. ПОРЯДОК ОКАЗАНИЯ УСЛУГИ**

**4.1.** Исполнитель приступает к оказанию Услуги в течение **3 (*трех*)** **рабочих дней** с момента поступления предоплаты на расчетный счет Исполнителя.

**4.2.** Для оказания Услуги Стороны выделяют по одному уполномоченному лицу до начала оказания Услуг с указанием фамилии, имени и отчества уполномоченных лиц,
их контактных данных, номеров телефонов и адресов электронной почты.

**4.3.** Исполнитель проводит сбор необходимой исходной информации для разработки политики информационной безопасности путем получения достоверной информации от Заказчика, а также проведения изучения объектов Заказчика и оценки существующего состояния информационной безопасности.

**4.4.** На основе полученных исходных данных, результатов изучений и оценки Исполнитель разрабатывает политику информационной безопасности, дает разъяснения Заказчику по выбранным мерам обеспечения информационной безопасности и согласовывает их с Заказчиком.

**4.5.** После разработки политики информационной безопасности Исполнитель направляет её Заказчику вместе с двумя экземплярами надлежащим образом оформленного Акта.

**4.6.** Заказчик, в течение **10 *(десяти)* календарных дней** после получения Акта обязан подписать его и один экземпляр направить Исполнителю, или направить Исполнителю мотивированный отказ от приемки оказанной Услуги. В случае необеспечения Заказчиком приемки оказанной Услуги и неполучения Исполнителем мотивированного отказа в течение **10 *(десяти)* календарных дней**, Услуга считается принятой Заказчиком.

**4.7.** В случае мотивированного отказа Заказчика от принятия оказанной Услуги, Сторонами составляется двухсторонний акт с перечнем необходимых доработок, и сроков их выполнения. После доработок Исполнитель вновь предъявляет Заказчику Услугу к приемке.

**5. КАЧЕСТВО УСЛУГИ**

**5.1**. Исполнитель гарантирует качественное оказание Услуги в соответствии
с требованиями Методики разработки политики информационной безопасности и настоящего Договора.

**5.2.** Качество оказанных Услуг Исполнитель подтверждает путём подписания Акта по результатам окончания оказываемой Услуги.

**6. КОНФИДЕНЦИАЛЬНОСТЬ**

**6.1.** Любые сведения и информация, полученная в ходе оказания Услуги, рассматриваются как конфиденциальная информация, которая не подлежит разглашению третьим лицам в соответствии с требованием законодательства Республики Узбекистан.

**6.2.**Условия настоящего Договора, дополнительных соглашений и иная информация, полученная Сторонами в соответствии с Договором, конфиденциальны и не подлежат разглашению.

**6.3.**Каждая из Сторон обязана обеспечить защиту конфиденциальной информации от несанкционированного использования, распространения или опубликования.

**6.4.** Условия конфиденциальности вступают в силу с момента подписания настоящего Договора.

**6.5.** Сторона, допустившая разглашение конфиденциальной информации либо не выполнившая иные требования по обеспечению ее конфиденциальности, несет ответственность в соответствии с законодательством Республики Узбекистан.

**6.6.**Любой ущерб, вызванный нарушением условий конфиденциальности, определяется и возмещается в соответствии с действующим законодательством Республики Узбекистан.

**6.7.**Конфиденциальная информация может предоставляться компетентным государственным органам в случаях и в порядке, предусмотренных действующим законодательством, что не влечет за собой наступление ответственности за её разглашение.

**7. ОТВЕТСТВЕННОСТЬ СТОРОН**

**7.1.** Заказчик несёт ответственность за достоверность информации, предоставляемой Исполнителю в качестве исходной информации для разработки политики информационной безопасности.

**7.2.** Стороны несут ответственность за нарушение обязательств в соответствии с действующим законодательством Республики Узбекистан и настоящим Договором.

**7.3.**За нарушение сроков оказания Услуги Заказчик вправе требовать
от Исполнителя уплаты пени в размере 0,5% от стоимости не оказанной в срок Услуги
за каждый день просрочки, но не более 50% данной стоимости.

**7.4.**За нарушение сроков оплаты Услуги Исполнитель вправе требовать
от Заказчика уплаты пени в размере 0,5% от суммы просроченного платежа за каждый день просрочки, но не более 50% от суммы просроченного платежа.

**7.5.** Сторона, для которой создалась невозможность исполнения обязательства
по Договору, вследствие форс-мажорных обстоятельств, должна в течение **5 *(пяти)*** **календарных** **дней** в письменной форме уведомить другую Сторону, как о наступлении, так и о прекращении действия таких обстоятельств.

**7.6.**Все другие видыответственности,не предусмотренные в настоящем Договоре, применяются в соответствии с действующим законодательством Республики Узбекистан.

**8. ПОРЯДОК ИЗМЕНЕНИЯ И РАСТОРЖЕНИЯ ДОГОВОРА**

8.1. Изменения и дополнения к данному Договору допускаются по взаимному согласию Сторон и оформляются отдельным дополнительным письменным соглашением, которое подписывается уполномоченными представителями Сторон и является неотъемлемой частью настоящего Договора.

8.2.Данный Договор может быть расторгнут по взаимному согласию Сторон или в одностороннем порядке по инициативе одной из Сторон путем направления письменного уведомления не менее чем за 10 *(десять)* календарных дней до даты его расторжения.

**8.3.**Датой расторжения Договора считается дата, указанная Стороной в уведомлении о расторжении Договора.

**8.4.** В случае прекращения действия Договора по инициативе Заказчика, оплата оказанной Услуги производится Заказчиком по фактическим затратам Исполнителя
в срок не позднее **5 *(пяти)*** **рабочих дней** с даты расторжения Договора.

**9. ДЕЙСТВИЕ ДОГОВОРА**

**9.1.** Настоящий договор вступает в силу с момента его подписания Сторонами и до полного его исполнения.

**9.2.** Отношения между Сторонами прекращаются при выполнении ими всех условий настоящего Договора и полного завершения расчетов.

**10. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ**

**10.1.** Все споры и разногласия, которые могут возникнуть между Сторонами
из Договора или в связи с ним, регулируются ими путем переговоров с применением претензионного порядка. При этом претензии рассматриваются, и ответ на них направляется в течение **15 *(пятнадцати)* календарных дней,** следующих за датой их поступления.

**10.2.** При не урегулировании споров и разногласий путем переговоров с применением претензионного порядка они подлежат разрешению в Ташкентском межрайонном Экономическом суде.

**11. ПРОЧИЕ УСЛОВИЯ**

**11.1.**Настоящий Договор составлен в двух подлинных экземплярах, имеющих равную юридическую силу, по одному для каждой из Сторон.

**11.2.**Каждая Сторона обязана письменно уведомить об изменении своих реквизитов (в том числе изменение адреса, банковских реквизитов и т.д.) в течение **5 *(пяти)* рабочих дней** с момента такого изменения.

**12. РЕКВИЗИТЫ И ПОДПИСИ СТОРОН**

|  |  |  |
| --- | --- | --- |
| **Заказчик:** |  | **Исполнитель:** |
|  |  |  |
|  |  | ГУП «Центр кибербезопасности»адр.: г.Ташкент, Мирабадский р-н,ул. Тараса Шевченко, д. 20 |
|  |  |  |
|  |  | *р/с: 2021 0000 4009 5333 9007* *«Алока Банк» АК Мирабадский филиал**МФО: 00401 ИНН: 305 907 639ОКЭД: 84112* |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **\_\_\_\_\_\_\_\_\_\_** |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**О. Мирзаев** |

Приложение

к Договору № \_\_\_\_\_\_

от «\_\_\_\_\_» \_\_\_\_\_\_\_\_ 20\_\_\_ г.

**Протокол**

**согласования цены на оказываемые Услуги**

Мы, нижеподписавшиеся, от Заказчика \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ и от Исполнителя Директор О. Мирзаев удостоверяем, что «Сторонами» достигнуто соглашение по величине договорной цены:

|  |  |  |
| --- | --- | --- |
| **№****п/п** | Состав работ | Цена, сум |
| **1** | **2** |  |
| **1** | Проведение предварительного обследования состояния информационной безопасности |
| 1.1 | Проведение инвентаризации, определение объектов защиты (информационные ресурсы, сети, ресурсы, технические средства обработки информации, помещения, где установлены и эксплуатируются эти средства, и предназначенные для ведения переговоров, в том числе конфиденциального характера) |
| 1.2 | Идентификация угроз информационной безопасности |
| 1.3 | Оценка принятых организационно-правовых мер защиты и используемых средств защиты информации |
| 1.4. | Определение рисков информационной безопасности |
| **2** | Разработка политики информационной безопасности |
| 2.1 | Указание целей и задач, объектов защиты, рисков и модели угроз информационной безопасности |
| 2.2 | Определение и указание мер информационной безопасности |
| 2.3. | Разработка документов, входящих в состав политики информационной безопасности (положения, инструкции, правила, перечней, порядков и планов) |
| 2.4. | Классификация информации и информационных ресурсов, разработка матриц доступа |
|  | **И Т О Г О: ( с учётом НДС)** | **8 875 694** |

Настоящий документ является неотъемлемой частью Договора и основанием для проведения взаимных расчетов между Исполнителем и Заказчиком.

|  |  |  |
| --- | --- | --- |
| **Заказчик:** |  | **Исполнитель:** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_ |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**О. Мирзаев** |