**Техническое задание**

**на выполнение работ по защите информации на объекте информатизации некоммерческой микрокредитной компании «Фонд развития малого и среднего предпринимательства Мурманской области» (НМКК «ФОРМАП» (Фонд))**

**Список используемых сокращений:**

|  |  |
| --- | --- |
| АС | Автоматизированная система |
| ИСПДн | Информационная система персональных данных |
| ИТ | Информационные технологии |
| ИТКС | Информационно- телекоммуникационные системы |
| КЗ | Контролируемая зона |
| ЛВС | Локально – вычислительная сеть |
| НСД | Несанкционированный доступ |
| ОВО | Отдел вневедомственной охраны |
| ОИ | Объект информатизации |
| ОРД | Организационно-распорядительная документация |
| ПДн | Персональные данные |
| ПО | Программное обеспечение |
| СЗИ | Система защиты информации |
| СрЗИ | Средства защиты информации |
| СЗПДн | Система защиты персональных данных |
| СУБД | Система управления баз данных |
| ТЗ | Техническое задание |
| ЧОП | Частное охранное предприятие |
| ФСБ | Федеральная служба безопасности |
| ФСТЭК | Федеральная служба по техническому и экспортному контролю |

**1. Наименование работ**

Выполнение комплекса мероприятий по защите информации ограниченного доступа.

**2. Правовое основание для осуществления поставки**

Услуги должны оказываться в соответствии со следующими нормативными правовыми актами:

* Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных»;
* Постановление Правительства РФ от 01.11.2012 № 1119 «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
* Приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
* Приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
* Методический документ «Методика оценки угроз безопасности информации», утв. ФСТЭК России 05.02.2021 г.;
* Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
* ГОСТ Р 50752 - 95. Информационная технология. Защита информации от утечки за счёт побочных электромагнитных излучений при её обработке средствами вычислительной техники. Методы испытаний;
* ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования;
* ГОСТ Р 50922-2006. Защита информации. Основные термины и определения;
* ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения;
* ГОСТ Р 52447-2005. Защита информации. Техника защиты информации. Номенклатура показателей качества;
* ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности;
* ГОСТ Р 51624 - 2000. Защита информации. Автоматизированные системы в защищённом исполнении. Основные требования;
* «Положение по аттестации объектов информатизации по требованиям безопасности информации», утв. Гостехкомиссии России 25.11.1994;
* Нормативно-методический документ. «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К), утверждённые приказом Гостехкомиссии России от 30.08.2002 № 282;
* «Сборник руководящих документов по защите информации от несанкционированного доступа» Гостехкомиссия России, Москва, 1998 г.;
* Профили защиты систем обнаружения вторжений. Утверждены директором ФСТЭК России 6 марта 2012;
* Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» (утв. решением Гостехкомиссии РФ 30 марта 1992 г.);
* Руководящий документ «Защита от несанкционированного доступа к информации», ч. 1 «Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия не декларируемых возможностей», Гостехкомиссия России, 1999 г.;
* Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации», Гостехкомиссия России, 1992 г.

**3. Состав и содержание работ исполнителя**

3.1. Обобщенный перечень мероприятий, предполагаемый на объекте информатизации:

|  |  |  |  |
| --- | --- | --- | --- |
| **Выполнение комплекса мероприятий по аттестации НМКК "ФОРМАП" (Фонд)** | | | |
| **№ п/п** | **Перечень оказываемых услуг** | **Результат оказываемых услуг** | **Количество** |
|  | Предпроектное обследование объекта информатизации. | Разработка и выдача аналитического обоснования необходимости создания системы защиты информации. | 1 |
|  | Техническое задание | Обоснование и детализация основных требований по защите информации ограниченного доступа в АИС на основании разработанной модели угроз и в соответствии с классом АИС | 1 |
| Разработка технического задания |
|  | Модель угроз безопасности информации | Разработка Модели (совокупности) угроз безопасности информации применительно к конкретным условиям функционирования объектов, подвергнутых предпроектному обследованию | 1 |
|  | Технический проект | Разработка проектных решений по СЗИ АИС в целом и ее частям | 1 |
|  | Поставка, установка и настройка средств защиты информации | Акт ввода в эксплуатацию СрЗИ | 1 |
|  | Ввод в действие | Подготовка объекта автоматизации к вводу СЗИ АИС | 1 |
| Подготовка персонала, инструктаж пользователей и администраторов по работе с комплексом средств защиты |
| Опытная эксплуатация СЗИ АИС в целях проверки их работоспособности в составе АИС | 1 |
| Проведение стендовых испытаний системы |
|  | Контроль эффективности внедрённых мер и средств защиты информации | Протокол оценки защищённости от НСД  Заключение по результатам контроля | 1 |

3.2. Содержание работ:

3.2.1. Предпроектная стадия, включающая обследование объекта и разработку аналитического обоснования необходимости создания системы защиты информации, включающая в себя:

определение границ обследования;

определение категорий ПДн и категорий субъектов ПДн;

определение целей обработки ПДн;

установление правовых оснований обработки;

определение соответствия целей обработки, способов обработки принципам обработки;

установление достаточности или избыточности ПДн для целей обработки;

определение срока, в течение которого производится обработка ПДн (в том числе и их хранение);

определение перечня действий с ПДн, которые производятся в ходе их обработки;

определение используемых оператором способов обработки ПДн;

изучение имевших место инцидентов информационной безопасности, связанных с ПДн;

изучение существующих организационных мер обеспечения безопасности ПДн;

определение наличия на предприятии документов, регламентирующих организацию и осуществление работ по защите информации (концепции, положения, руководства, приказы, стандарты, регламенты, инструкции и др.);

уточнение структуры подразделений предприятия, участвующих в организации и осуществлении работ по защите информации (лиц ответственных за безопасность информации);

уточнение организации учета носителей защищаемой информации;

анализ документации Заказчика, регламентирующей обработку ПДн;

определение перечня (состава) ПДн, обрабатываемых на каждой из технологических площадок;

определение исходных данных для классификации ИСПДн НМКК "ФОРМАП";

определение состава и структуры защищаемых ИСПДн НМКК "ФОРМАП" в том числе:

определение количества АРМ, серверов и коммутационного оборудования, участвующих (либо планируемых к внедрению) в процессе обработки ПДн;

сбор данных о структуре общесистемного и прикладного программного обеспечения в ИС НМКК "ФОРМАП" (включая СУБД и средства модификации объектного кода программ) с указанием сертификатов ФСТЭК России и/или ФСБ России (при их наличии);

сбор данных о составе и структуре СЗПДн (применяемые СрЗИ: средства защиты от НСД, антивирусные средства, межсетевые экраны, средства обнаружения вторжений, криптографические средства и др. с указанием сертификатов ФСТЭК России и/или ФСБ России (при их наличии)).

определение конфигурации и топологии ИСПДн НМКК "ФОРМАП" в целом и их отдельных компонент, физических, функциональных и технологических связей как внутри системы, так и с другими системами различного уровня и назначения;

сбор сведений о наличии физической охраны технических средств ИСПДн НМКК "ФОРМАП" (собственная Служба безопасности, ЧОП, ВОХР ОВО МВД и т.п.), применении технических средств охраны (охранно-пожарная сигнализация, СКУД, видеонаблюдение и др.), а также режиме охраны (круглосуточно, только в нерабочее время и т.п.);

изучение технологических процессов обработки ПДн;

комплексное обследование ОИ, условий их размещения, режимов функционирования, определение общего и специального ПО;

классификация ОИ, обрабатывающих ПДн. Проведение исследований угроз безопасности персональных данных, оценку исходной защищенности ОИ.

3.2.2. Разработать «Модель угроз безопасности» по требованиям безопасности информации, в том числе (основание оказания услуги в соответствии с требованиями Постановления Правительства от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и требованиями Приказа ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»):

* произвести оценку угроз безопасности информации ИСПДн НМКК "ФОРМАП";
* определить негативные последствия от реализации (возникновения) угроз безопасности информации;
* произвести оценку возможности реализации (возникновения) угроз безопасности информации и определить их актуальность;
* произвести оценку актуальности угроз безопасности информации.

3.2.3. Разработать техническое (частное техническое) задание на создание СЗИ (основание оказания услуги Руководящий документ Гостехкомиссии России «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» утвержденные приказом Гостехкомиссии России от 30.08.2002 № 282 п.п. 3.18).

Техническое (частное техническое) задание должно содержать:

* обоснование разработки;
* исходные данные создаваемого (модернизируемого) объекта информатизации в техническом, программном, информационном и организационном аспектах;
* класс защищенности АС;
* ссылку на нормативные документы, с учетом которых будет разрабатываться СЗИ и приниматься в эксплуатацию объект информатизации;
* конкретизацию требований к СЗИ на основе действующих нормативно-методических документов и установленного класса защищенности АС;
* перечень предполагаемых к использованию сертифицированных средств защиты информации;
* обоснование проведения разработок собственных средств защиты информации, невозможности или нецелесообразности использования, имеющихся на рынке сертифицированных средств защиты информации;
* состав, содержание и сроки проведения работ по этапам разработки и внедрения;
* перечень подрядных организаций-исполнителей видов работ;
* перечень предъявляемой заказчику научно-технической продукции и документации.

3.2.4. Разработать проект на создание СЗПДн в ИСПДн НМКК "ФОРМАП" (основание оказания услуги Руководящий документ Гостехкомиссии России «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)» утвержденные приказом Гостехкомиссии России от 30.08.2002 № 282 п.п. 3.16-3.18).

Проект должен содержать:

* пояснительную записку с изложением решений по комплексу организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации, состава средств защиты информации с указанием их соответствия требованиям ТЗ;
* описания технического, программного, информационного обеспечения и технологии обработки (передачи) информации;
* плана организационно-технических мероприятий по подготовке объекта информатизации к внедрению средств и мер защиты информации.

3.2.5. Осуществить поставку, установку и настройку СрЗИ в соответствии с требованиями Приложения № 1 к настоящему техническому заданию.

3.2.7. Провести опытную эксплуатацию внедряемых СрЗИ на выделенном сегменте ЛВС.

* конфигурирование и интеграция СЗИ НСД в существующую инфраструктуру ИСПДн НМКК "ФОРМАП";
* проведение эксплуатационно- технических испытаний применённых СрЗИ по проверке совместимости параметров их конфигурации с программной средой исполнения;
* расширенный инструктаж пользователей ИСПДн НМКК "ФОРМАП" базовым знаниям по основам защищенной обработки персональных данных с учетом внедренных организационных и технических мер, в т.ч. с использованием комплекта организационно-распорядительных и эксплуатационно-технических документов.

3.2.8. Проведение комплексных испытаний ИСПДн НМКК "ФОРМАП", c разработкой протокола оценки соответствия СЗПДн, заключения по результатам оценки в том числе:

* анализ уязвимостей ИСПДн НМКК "ФОРМАП", в том числе вызванных ошибками в конфигурировании программного обеспечения и средств защиты информации;
* испытания подсистемы обеспечения информационной безопасности ИСПДн НМКК "ФОРМАП" путем осуществления попыток несанкционированного доступа к ИСПДн НМКК "ФОРМАП" в обход подсистемы обеспечения информационной безопасности.

**4. Требования к документированию**

Каждая стадия оказания услуг должна сопровождаться разработкой исполнительной документации, согласно нормативным требованиям и требованиям, указанным в настоящей документации.

4.1. Аналитическое обоснование должно содержать:

* информационную характеристику и организационную структуру объекта информатизации;
* характеристику комплекса основных и вспомогательных технических средств, программного обеспечения, режимов работы, технологического процесса обработки информации;
* возможные каналы утечки информации и перечень мероприятий по их устранению и ограничению;
* перечень предлагаемых к использованию сертифицированных средств защиты информации;
* обоснование необходимости привлечения специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации;
* оценку материальных, трудовых и финансовых затрат на разработку и внедрение СЗИ;
* ориентировочные сроки разработки и внедрения СЗИ.

4.2. Модель угроз безопасности должна содержать:

* структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования;
* оценку возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализ возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности);
* перечень актуальных угроз безопасности информации.

Модель нарушителя должна содержать:

* описание совокупности предположений о возможностях нарушителя, которые он в состоянии использовать для разработки и проведения атак, а также об ограничениях на эти возможности;
* определение требуемого класса средств криптографической защиты информации (далее – СКЗИ).

4.3. Техническое задание на создание СЗИ должно содержать:

* обоснование разработки;
* исходные данные создаваемого (модернизируемого) объекта информатизации в техническом, программном, информационном и организационном аспектах;
* класс защищенности АС;
* ссылку на нормативные документы, с учетом которых будет разрабатываться СЗИ и приниматься в эксплуатацию объект информатизации;
* конкретизацию требований к СЗИ на основе действующих нормативно-методических документов и установленного класса защищенности АС;
* перечень предполагаемых к использованию сертифицированных средств защиты информации;
* обоснование проведения разработок собственных средств защиты информации, невозможности или нецелесообразности использования, имеющихся на рынке сертифицированных средств защиты информации;
* состав, содержание и сроки проведения работ по этапам разработки и внедрения;
* перечень подрядных организаций-исполнителей видов работ;
* перечень предъявляемой заказчику научно-технической продукции и документации.

4.4. Проект на создание СЗПДн должен содержать:

* общую информацию об организации;
* информацию о физической безопасности ИСПДн;
* описание технологических процессов обработки ПДн;
* описание ИСПДн;
* аналитическое обоснование выбранных мер для реализации СЗПДн;
* описание вариантов реализации СЗПДн;
* технический проект.

4.5. По результатам установки и настройки СрЗИ Исполнитель передаёт Заказчику:

* эксплуатационную и техническую документацию на внедрённые СрЗИ;
* акты установки и настройки СрЗИ.

**5. Требования к Исполнителю**

Исполнитель должен обладать следующими действующими на момент заключения договора разрешительными документами:

* Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации (обоснование необходимости лицензии: Федеральный закон «О лицензировании отдельных видов деятельности» от 04.05.2011 г № 99-ФЗ, ст.12, п.1,пп.5)

Перечень работ и услуг, на которые должна распространяться настоящая лицензия:

* аттестационные испытания и аттестация на соответствие требованиям по защите информации;
* проектирование в защищенном исполнении: средств и систем информатизации; помещений со средствами (системами) информатизации, подлежащими защите; защищаемых помещений;
* контроль защищенности конфиденциальной информации от утечки по техническим каналам в: средствах и системах информатизации; технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещенных в помещениях, где она обрабатывается; помещениях со средствами (системами), подлежащими защите; защищаемых помещениях;
* контроль защищённости конфиденциальной информации от несанкционированного доступа и её модификации в средствах и системах информатизации
* установка, монтаж, наладка, испытания, ремонт средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).
* Лицензия ФСБ России на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя). (обоснование необходимости лицензии: Федеральный закон «О лицензировании отдельных видов деятельности» от 04.05.2011 г № 99-ФЗ, ст.12, п.1,пп1).

Перечень работ и услуг, на которые должна распространяться настоящая лицензия:

* Разработка защищенных с использованием шифровальных (криптографических) средств информационных систем;
* Разработка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* Монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств, за исключением шифровальных (криптографических) средств защиты фискальных данных, разработанных для применения в составе контрольно-кассовой техники, сертифицированных Федеральной службой безопасности Российской Федерации;
* Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем;
* Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;
* Монтаж, установка (инсталляция), наладка средств изготовления ключевых документов;

Работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

**6. Технические условия.**

6.1. Все сведения, необходимые для оказания услуг, Исполнитель получает лично у представителя Заказчика по адресу: 183031, г. Мурманск, Подстаницкого, 1

6.2. Все услуги оказываются Исполнителем исключительно на территории нахождения Заказчика согласно месту оказания услуг при личном очном присутствии специалистов по информационной безопасности в соответствии с местом оказания услуг. Удаленное оказание даже части услуг в том числе с применением методов удаленной работы недопустимо. Прочие расходы Исполнителя учитываются Исполнителем при подаче заявки и дополнительно Заказчиком не оплачиваются.

6.3. Заказчик вправе провести экспертизу приемки выполняемых работ с привлечением сторонней экспертной организации.

В случае выявления несоответствия оказанных услуг требованиям Технического здания, расходы независимой экспертизы оплачиваются Исполнителем.

6.4. Комплект документов предоставляется Заказчику в твердой копии, в одном экземпляре, посредством передачи по специальной (фельдъегерской) почте.

6.5. Исполнитель принимает на себя обязательства по предоставлению гарантии качества на результат оказанных услуг. Срок предоставления гарантии качества оказания услуг – 12 (Двенадцать) месяцев с даты подписания Сторонами Акта сдачи-приемки оказанных услуг.

6.6. Исполнитель несет ответственность за обнаруженные недостатки в период гарантийного срока. В случае выявления недостатков в гарантийный период Исполнитель безвозмездно выполняет работы по их устранению. Срок устранения недостатков устанавливается Заказчиком, но не должен превышать 1 (Одного) месяца с момента выявления недостатков.

**7. Требования к обеспечению безопасности в ходе разработки и внедрения СЗПДн.**

Все сведения о составе и характеристиках СЗПДн являются конфиденциальной информацией.

Разработчик СЗПДн обязуется:

- не проводить противозаконные действия по сбору, использованию и передаче третьей стороне информации циркулирующей и хранящейся в ИС;

- не осуществлять несанкционированный доступ к информационным ресурсам ИС;

- не проводить незаконное копирование информации, циркулирующей или хранящейся в ИС;

- не предпринимать манипулирование информацией, циркулирующей или хранящейся в ИС (фальсифицировать, модифицировать, подделывать, блокировать, уничтожать или искажать информацию);

- не нарушать технологию сбора, накопления, хранения, обработки, преобразования, отображения и передачи информации, в результате чего может быть осуществлено искажение, потеря или незаконное использование информации;

- не внедрять в ИС программы-вирусы (загрузочные, файловые и др.);

- не устанавливать программные и аппаратные закладные устройства в технические средства ИС;

- не устанавливать в технические средства ИС программное обеспечение, зараженное вирусами;

- не привлекать третьих лиц (соисполнителей/ субподрядчиков) для осуществления предоставления лицензионных прав, а также для выполнения работ по настоящему техническому заданию.

Нарушение настоящих требований влечет за собою гражданско-правовую, административную или уголовную ответственность в соответствии с законом Российской Федерации.

Приложение № 1

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование товара** | **Характеристики товара** | **Кол-во, шт.** |
|  | **Право на использование Единого центра управления для Dallas Lock до 99 рабочих станций.**  **Бессрочная лицензия.** | ЕЦУ – единый центр управления средствами защиты информации от несанкционированного доступа должен выполнять следующие функции:   * контроль состояния (целостности настроек) активного сетевого оборудования. ЕЦУ идентифицирует сетевое оборудование как объекты домена безопасности и позволяет осуществлять мониторинг изменений конфигурации по протоколу SNMP для таких объектов.   Особенности:  • поддержка разных версий протокола (SNMPv1,SNMPv2c, SNMPv3);  • сканирование сети для обнаружения активных SNMP-клиентов;  • контроль целостности конфигурации активного сетевого оборудования, в том числе отдельных параметров на основе OID;  • сигнализация о нарушении целостности;  • поддержка собственной расширяемой базы конфигурационных файлов.  • ЕЦУ позволяет создавать иерархическую структуру доменов безопасности с наследованием значений параметров безопасности. Дерево доменов безопасности может быть сколько угодно большим и сложным.  Переключение между настройками каждого домена безопасности происходит интуитивно понятно.  • ЕЦУ является кроссплатформенным решением и совместим с ОС семейств Windows и Linux. Работоспособность обеспечивается в том числе на российских дистрибутивах: Astra Linux Common Edition (релиз «Орел»), Astra Linux Special Edition (релиз «Смоленск»), Альт Рабочая станция. Список поддерживаемых ОС постоянно пополняется;  • ЕЦУ позволяет управлять СЗИ на клиентских АРМ, находящиИСя за NAT. | **1** |
|  | **Право на использование средства защиты информации от несанкционированного доступа**  **Dallas Lock 8.0-K** | 1. Средство защиты информации от несанкционированного доступа (СЗИ НСД) должно представлять собой программный комплекс средств защиты информации в операционных системах семейства Windows и Linux с возможностью подключения аппаратных идентификаторов. 2. СЗИ НСД должна быть предназначена для ПЭВМ типа IBM PC под управлением операционных систем Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Ubuntu 16.04 x64 (версия ядра 4.4), Debian 7.11 x64 (версия ядра 3.18), Red Hat Enterprise Linux Server 7 x64 (версия ядра 4.4, 3.18), Fedora 24 x64 (версия ядра 4.4, 3.18), OpenSUSE 42 x64 (версия ядра 4.4), CentOS 7 x64 (версия ядра 4.4, 3.18 х64 в многопользовательском режиме их эксплуатации. 3. СЗИ НСД должна поддерживать 32- и 64-битные версии операционных систем семейства Windows и 64-битные версии операционных систем семейства Linux. 4. СЗИ НСД должна быть предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках, планшетах), серверах, также поддерживать виртуальные среды. 5. СЗИ НСД должна обеспечивать:    1. регистрацию различных пользователей: локальных, доменных, сетевых. Определение количества одновременных сеансов для пользователя. Возможность ограничения количества терминальных сессий на одном компьютере;    2. идентификацию и проверку подлинности пользователей при входе в операционную систему. Возможность двухфакторной идентификации по паролю и аппаратному идентификатору. Возможность задать расписание работы пользователей. Возможность записи авторизационных данных в идентификатор. Возможность определить принадлежность аппаратного идентификатора конкретному пользователю. Поддержку входа в ОС по сертификату смарт-карты, выданному удостоверяющим центром в ОС семейства Windows;    3. реализацию настроек сложности паролей и механизм генерации пароля, соответствующего настройкам;    4. возможность автоматического выбора аппаратного идентификатора в окне авторизации при входе в операционную систему;    5. возможность настройки принудительной двухфакторной аутентификации для учётной записи с правами администратора и/или пользователя;    6. возможность средствами СЗИ НСД выполнить настройку периода действия учётной записи;    7. возможность настройки предупреждения пользователя до входа в систему о том, что в информационной системе реализованы меры по обеспечению безопасности информации;    8. возможность при создании учётной записи выбрать тип учётной записи (внутренний, внешний, системный, приложение, гостевой, временный);    9. независимый от механизмов ОС механизм разграничения прав доступа к объектам файловой системы, к запуску программ и к печати документов. Разграничения должны касаться доступа к объектам файловой системы (FAT и NTFS), реестру, сети, съемным носителям информации. Разграничения должны касаться всех пользователей – локальных, сетевых, доменных, терминальных;    10. контроль аппаратной конфигурации компьютера и следующих подключаемых устройств:   – Android-устройств;  – iOS-устройств;  – Bluetooth-устройств;  – DVD- и CD-ROM-дисководов;  – устройств HID, MTD, PCMCIA, IEEE 1394, Secure Digital;  – USB-контроллеров;  – беспроводных устройств (Wireless Communication Devices);  – биометрических устройств;  – дисководов магнитных дисков;  – звуковых, видео- и игровых устройств;  – инфракрасных устройств (IrDA);  – контроллеров магнитных дисков;  – ленточных накопителей;  – модемов;  – переносных устройств;  – портов (COM и LPT);  – сенсоров;  – сетевых адаптеров;  – сканеров и цифровых фотоаппаратов;  – принтеров;  – съемных носителей информации (CD-ROM, FDD, USB-Flash-накопителей).   * 1. контроль устройств, подключаемых к терминальному серверу с RDP-клиентов (контроль перенаправления устройств);   2. предотвращение утечки информации с использованием съемных носителей информации. СЗИ НСД должна позволять разграничивать доступ как к отдельным типам носителей, так и к конкретным экземплярам;   3. преобразование информации:   – при работе с виртуальными дисками (преобразование выполняется незаметно для пользователя);  – при создании преобразованных файлов-контейнеров, используемых для хранения информации на внешних носителях или для передачи по различным каналам связи.   * 1. блокировку виртуальных дисков с преобразованной информацией при отключении аппаратного идентификатора;   2. возможность работы с преобразованными файлами-контейнерами на компьютерах, где программное обеспечение СЗИ НСД не установлено;   3. сохранение теневых копий файлов, записываемых на съемные носители;   4. автоматическое ограничение доступа к теневой копии, сделанной СЗИ НСД при копировании секретного документа на сменный машинный носитель;   5. использование дискреционного принципа контроля доступа:   – обеспечивает доступ к защищаемым объектам (дискам, каталогам, файлам) в соответствии со списками пользователей (групп) и их правами доступа (матрица доступа).   * 1. возможность ограничивать средствами СЗИ НСД круг доступных сетевых ресурсов (с точностью до отдельных удаленных рабочих станций и отдельных папок общего доступа);   2. регистрацию и учет (аудит) действий пользователей независимыми от ОС средствами (включение ПЭВМ, вход/выход пользователей, доступ к ресурсам, запуск/остановка процессов, администрирование). Должны вестись непрерывные журналы (т. е. новые записи не должны затирать более старые) с возможностью сортировки и архивации записей;   3. расширенные возможности аудита печати: печать документов с возможностью добавления штампа (произвольного или по ГОСТ), возможность сохранения теневых копий распечатываемых документов, разграничение доступа пользователей к печати и нанесению штампов;   4. возможность организации замкнутой программной среды (ЗПС) и различные способы ее настройки;   5. возможность разграничения доступа к буферу обмена;   6. возможность локального и удаленного администрирования (управление учетными записями, политиками безопасности, правами доступа, аудитом, просмотр журналов);   7. возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию. А также контроль целостности файлов при доступе и блокировка входа в ОС при выявлении изменений. Возможность восстановления объекта доступа (файла, ветки реестра) в случае обнаружения нарушения его целостности;   8. очистку остаточной информации (освобождаемого дискового пространства, зачистку определенных файлов и папок по команде пользователя), а также возможность полной зачистки дисков и разделов. Возможность определения метода зачистки. Контроль зачистки при полной зачистке логического диска. Запрет смены пользователей без перезагрузки;   9. выполнение регистрации действий по зачистке остаточной информации;   10. возможность самодиагностики основного функционала СЗИ НСД с возможностью сохранения отчета;   11. возможность сохранения конфигурации для последующего восстановления СЗИ НСД;   12. ведение двух копий программных средств защиты информации и возможность возврата к настройкам по умолчанию;   13. возможность нотификации о наличии обновлений для СЗИ НСД на сервере компании-разработчика СЗИ НСД;   14. возможность использования SQL базы данных для централизованного хранения событий аудита;   15. возможность сигнализации администратору безопасности о ситуациях несанкционированного доступа на клиентских рабочих станциях:   – нарушение контроля целостности объекта;  – попытка работы после блокировки при нарушении целостности;  – попытка входа на клиентскую рабочую станцию с неправильным паролем;  – блокировка пользователя после многократного ввода неправильного пароля;  – СЗИ НСД на клиенте не отвечает (возможная причина - несанкционированная деактивация системы защиты);  – клиент недоступен долгое время (с возможностью задания периода времени);  – попытки монтирования и попытка работы с запрещенными для пользователей на клиенте устройствами.   * 1. блокировку доступа к файлам по расширению;   2. возможность настройки всех параметров СЗИ НСД из единой консоли администрирования;   3. возможность создания отчета по назначенным правам, формирование паспорта программного обеспечения, установленного на ПЭВМ, формирование паспорта аппаратной части ПЭВМ;   4. возможность построения иерархии управления при помощи специального модуля – менеджера, управляющего несколькими модулями централизованного управления;   5. возможность использования механизма удаленной установки и обновления СЗИ НСД средствами модуля централизованного управления самой СЗИ или средствами групповых политик Active Directory. Проверка подписи файлов при обновлении СЗИ НСД;   6. возможность визуализации сети защищаемых компьютеров;   7. возможность подключения к модулям администрирования пользователя с ограниченными правами (права только на просмотр настроек; только на просмотр журналов аудита; полные права с возможностью делегирования);   8. возможность выполнять синхронизацию времени между сервером безопасности и клиентами;   9. возможность интеграции с SIEM-системами;   10. возможность интеграции с антивирусными системами.  1. Реализация СЗИ НСД должна быть полностью программной с возможностью подключения аппаратных средств считывания индивидуальных идентификаторов пользователей, включая идентификаторы:   – USB-Flash-накопители;  – электронные ключи Touch Memory (iButton);  – USB-ключи Aladdin eToken Pro/Java;  – смарт-карты Aladdin eToken Pro/SC;  – USB-ключи Rutoken и Rutoken ЭЦП, смарт-карты Rutoken;  – JaCarta ГОСТ/PKI (USB-ключи и смарт-карты);  – карты HID Proximity;  – USB-токен и смарт-карты ESMART Token (ESMART Token ГОСТ);  – NFC-метки.  Поставка СЗИ НСД должна осуществляться в форме передачи неисключительных прав на использование программного обеспечения с указанием всех необходимых модулей и требуемого количества лицензий по каждому модулю. | **50** |
|  | **Аппаратная платформа UserGate С100 в составе:**  **Лицензия для UserGate**  **без ограничений количества пользователей**  **Модуль Advanced**  **Threat Protection на 1 год для UserGate**  **без ограничений числа пользователей;**  **Модуль Mail Security на**  **1 год для UserGate**  **без ограничений количества пользователей**  **Модуль Stream Antivirus на 1 год**  **без ограничений количества пользователей** | UserGate С100 межсетевой экран оснащенный 5 портами 10/100/1000Base-T обеспечивает пропускную способность до 2000 UDP  (Mбит/с), инспектирует SSL до 70 (Mбит/с), Потоковый антивирус, до 200 (Мбит/с), поддерживает функционал:   * Межсетевой экран * Система обнаружения вторжений (IDS/IPS) * Доступ к внутренним ресурсам через SSL VPN Portal * Анализ и выгрузка информации об инцидентах безопасности (SIEM) * Автоматизация реакции на угрозы безопасности информации (SOAR) * Обратный прокси * Контроль доступа в интернет * Контроль Приложений L7 * Дешифрование SSL * Гостевой портал * Безопасная публикация внутренних ресурсов и сервисов * Антивирусная защита * Advanced Threat Protection * Безопасность почты * Идентификация пользователей * Поддержка концепции BYOD (Bring Your Own Device) * Виртуальная частная сеть (VPN) * Удаленное администрирование * Поддержка АСУ ТП (SCADA) | **1** |