****

**Федеральная нотариальная палата**

**Фонд  «Центр инноваций и информационных технологий»**

**Проект**

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ**

Технические мероприятия по обеспечению безопасности персональных данных при осуществлении нотариальной деятельности

**Версия 1.0**

**Москва 2010**

**Содержание:**

|  |  |  |
| --- | --- | --- |
|  | **Общие положения** |  |
|  | * 1. **Цели и задачи** |  |
|  | * 1. **Область применения** |  |
|  | * 1. **Термины и определения** |  |
|  | * 1. **Нормативно-правовая база** |  |
|  | **Объекты защиты ИСПДн.** |  |
| **3.** | **Общие требования к СиЗИ ИСПДн** |  |
| **4.** | **Рекомендации по выбору программно-аппаратных СЗИ** |  |
| **5.** | **Краткий обзор программно-аппаратных средств защиты информации , применимых для создания ИСПДн. в защищенном исполнении** |  |
| **6.** | **Сравнительный анализ программно-аппаратных средств защиты информации , применимых для создания ИСПДн. в защищенном исполнении.** |  |
| **7.** | **Типовые варианты системы защиты ПДн. в ИСПДн.** |  |
| **8.** | Технические требования, предъявляемые к рабочим станциям с установленными средствами защиты |  |
| **9.** | **Рекомендации по оптимизации затрат на создание СиЗИ ИСПДн** |  |
| **10.** | **Заключение** |  |

1. **Общие положения**

**1.1. Цели и задачи**

Методические рекомендации. Технические мероприятия по обеспечению

безопасности персональных данных при осуществлении нотариальной деятельности (далее Методические рекомендации), разработаны Фондом  «Центр инноваций и информационных технологий» Федеральной нотариальной палаты с целью:

* методического обеспечения работ по приведению информационных систем персональных данных (далее ИСПДн.), применяемых для обработки персональных данных (далее ПДн.) при осуществлении нотариальной деятельности, в соответствие с требованиями Федерального Закона РФ № 152 «О персональных данных»;
* оптимизации затрат на внедрение программно-технических решений по защите ПДн.

Для достижения указанных целей необходимо решить следующие задачи:

* определить объекты защиты в ИСПДн.;
* провести сравнительный анализ программно-аппаратных средств защиты информации (далее СЗИ), применимых для создания ИСПДн. в защищенном исполнении;
* разработать типовые варианты системы защиты ПДн. в ИСПДн.;
* разработать рекомендации по выбору программно-аппаратных СЗИ;
* разработать рекомендации по оптимизации затрат на создание СиЗИ ИСПДн;

**1.2. Область применения**

Методические рекомендации предназначены для специалистов по обеспечению

безопасности информации, руководителей, лиц ответственных за организацию и обеспечение режима информационной безопасности в ИСПДн.

Действие настоящих Методических рекомендаций не распространяется на

отношения, возникающие при:

* обработке ПДн, осуществляемой без использования средств автоматизации. В этом случае правила обработки ПДн определяются требованиями «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.
* обработке ПДн физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов ПДн;
* организации хранения, комплектования, учета и использования, содержащих ПДн документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;

**1.3. Термины и определения**

В настоящих методических рекомендациях используются следующие основные понятия:

**Автоматизированная система (AC)** - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (ГОСТ 34.003-90).

**Автоматизированное рабочее место (АРМ)** - программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида (ГОСТ 34.003-90).

**Администратор информационной безопасности [Администратор защиты] (АИБ) -** субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации (Гостехкомиссия России. РД. Защита от несанкционированного доступа к информации. Термины и определения).

**Администратор системы (системный администратор)** - лицо, отвечающее за эксплуатацию системы и поддержание ее в работоспособном состоянии.

**База данных - э**то объективная форма представления и организации совокупности данных (статей, расчетов и т.д.), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ) (закон «О правовой охране программ для ЭВМ и баз данных»).

**Безопасность информации [данных] -**  Состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность (ГОСТ Р 50922-2006).

**Блокирование персональных данных -** блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи (ФЗ №152).

**Вредоносные программы -** программы, предназначенные для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы (ГОСТ Р 50922-2006).

### Данные - факты, понятия или команды, представленные в формализованном виде и позволяющие осуществлять их передачу или обработку как вручную, так и с помощью средств автоматизации (ГОСТ Р 50922-2006).

**Защита информации (ЗИ)** - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию (ГОСТ Р 50922-2006).

**Защита информации от несанкционированного воздействия (ЗИ от НСВ)** - защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации (ГОСТ Р 50922-2006).

**Защита информации от непреднамеренного воздействия (ЗИ НПВ) -** защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации (ГОСТ Р 50922-2006).

**Защита информации от разглашения -** защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации (ГОСТ Р 50922-2006).

**Защита информации от несанкционированного доступа (ЗИ от НСД)** - защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации ( ГОСТ Р 50922-2006).

**Защита информации от преднамеренного воздействия** **(ЗИ от ПДВ)** - защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях (ГОСТ Р 50922-2006).

**Информационная система** **(ИС)** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (Федеральный закон № 149 «Об информации, информационных технологиях и защите информации»).

**Информационная система персональных данных (ИСПДн.)** - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств (ФЗ №152).

**Информационная технология (ИТ)** - приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, обработки, хранения, обработки, передачи и использования данных (ГОСТ 34.003-90).

**Информация -** сведения (сообщения, данные) независимо от формы их представления (ФЗ №149).

**Использование персональных данных** - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц (ФЗ №152);

**Конфиденциальность персональных данных** - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания (ФЗ №152);

**Криптографическая защита информации -** защита информации с помощью ее криптографического преобразования (ГОСТ Р 50922-2006).

**Межсетевой экран (МЭ)** - представляет собой локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС (ФСТЕК, РД Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.).

**Модель угроз (безопасности информации) -** физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации (ГОСТ Р 50922-2006).

**Нарушитель правил разграничения доступа** - субъект доступа, осуществляющий несанкционированный доступ к информации (Гостехкомиссия России. РД. Защита от несанкционированного доступа к информации. Термины и определения.).

**Носитель информации** - Материальный объект, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин (ГОСТ Р 50922-2006).

**Обезличивание персональных данных** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных (ФЗ №152).

**Обработка персональных данных -** действия (операции) с персональными данными, включающие сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных (ФЗ №152).

**Общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности (ФЗ №152).

**Оператор -** государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных (ФЗ №152).

**Персональные данные (ПДн.) - л**юбая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация (ФЗ №152).

**Политика безопасности (информации в организации) -** совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности (ГОСТ Р 50922-2006).

**Правило доступа к информации (правило доступа) -** совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям (ГОСТ Р 50922-96).

**Распространение персональных данных** - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом (ФЗ № 152).

**Система защиты информации (СиЗИ) -**  совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации (ГОСТ 34.003-90).

**Средство защиты информации (СЗИ)** - техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации ( ГОСТ Р 50922-2006).

**Сертификация на соответствие требованиям по безопасности информации -** форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров (ГОСТ Р 50922-2006)..

**Специальные информационные системы** - информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий) (ФЗ №152).

**Техническая защита информации (ТЗИ)** - Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств (ГОСТ Р 50922-2006).

**Типовые информационные системы -** информационные системы, в которых требуется обеспечение только конфиденциальности персональных данных (ФЗ №152).

**Трансграничная передача персональных данных -** передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства (ФЗ №152).

**Угроза (безопасности информации) -** Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации (ГОСТ Р 50922-2006).

**Уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных (ФЗ №152).

**Физическая защита информации -** Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты (ГОСТ Р 50922-2006).

**Целостность информации** - Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения) (Гостехкомиссия России. РД. Защита от несанкционированного доступа к информации. Термины и определения).

**1.4. Нормативно-правовая база**

Настоящие Методические рекомендации разработаны на основании следующих нормативно-правовых актов РФ:

1. Указа Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера»;
2. Федерального закона от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
3. Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
4. Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
5. Положения об обеспечении безопасности персональных данных при их обработке в

информационных системах персональных данных, утвержденного постановлением

Правительства Российской Федерации от 17 ноября 2007 г. № 781;

1. Постановления Правительства Российской Федерации от 15 сентября 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
2. Приказа Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»
3. Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 г.;
4. Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14 февраля 2008 г.;
5. Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации ФСБ (утверждены руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/54–144–);
6. Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/6/6-622);
7. Приказа ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

Методы и способы защиты персональных данных, содержащиеся в настоящих

методических рекомендациях, могут уточняться и дополняться по мере их реализации и совершенствования нормативно-правовой базы Российской Федерации в области защиты информации.

Внесение изменений в Методические рекомендации осуществляется в порядке,

устанавливаемом **Фондом  «Центр инноваций и информационных технологий»**.

1. **Объекты защиты ИСПДн.**

**Объектами защиты являются** – информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты.

Перечень объектов защиты определяется по результатам [проведения внутренней проверки](Приложение%208%20Отчет%20о%20результатах%20проведения%20внутренней%20проверки.doc).

Объекты защиты каждой ИСПДн могут включать:

1. **Персональные данные субъектов ПДн и сотрудников**

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация (ФЗ 152)

1. **Технологическая информация**

Технологическая информация, подлежащая защите, может включать:

* управляющую информацию (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
* технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
* информацию на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
* информацию о СиЗи ИСПДн, их составе и структуре, принципах и технических решениях защиты;
* информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
* служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки Обрабатываемой информации.

1. **Программно-технические средства обработки**

Программно-технические средства могут включать в себя:

* общесистемное и специальное программное обеспечение (операционные системы, СУБД, клиент-серверные приложения и другие);
* резервные копии общесистемного программного обеспечения;
* инструментальные средства и утилиты систем управления ресурсами ИСПДн;
* аппаратные средства обработки ПДн (АРМ и сервера);
* сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.).

1. **Средства защиты ПДн.**

Средства защиты ПДн состоят из аппаратно-программных средств, и могут включать:

* средства управления и разграничения доступа пользователей;
* средства обеспечения регистрации и учета действий с информацией;
* средства, обеспечивающие целостность данных;
* средства антивирусной защиты;
* средства межсетевого экранирования;
* средства аудита безопасности;
* средства обнаружения вторжений;
* средства криптографической защиты ПДн, при их передачи по каналам связи сетей общего и (или) международного обмена;
* средства управления процессами обеспечения безопасности;
* средства защиты информации от утечки по техническим каналам.

1. **Каналы информационного обмена и телекоммуникации.**

Каналы информационного обмена и телекоммуникации являются объектами защиты, если по ним передаются обрабатываемая и технологическая информация.

1. **Объекты и помещения, в которых размещены компоненты ИСПДн.**

Объекты и помещения являются объектами защиты, если в них происходит обработка обрабатываемой и технологической информации, установлены технические средства обработки и защиты.

### Анализ типовой схемы документооборота, применяемой при осуществлении

### нотариальной деятельности, позволил разработать типовую структурную схему автоматизированной ИСПДн. (рис. 1).

### В соответствии с данной схемой предлагается выделить 3 базовых уровня информационного взаимодействия, на которых осуществляется автоматизированная обработка ПДн.:

### уровень автоматизированного рабочего места пользователей (АРМ),

### уровень внутрисетевого взаимодействия,

### уровень межсетевого взаимодействия.



**Рис.1.**

1. **Общие требования к СиЗИ ИСПДн**

Система защиты персональных данных (СиЗИ ПДн.), строится на основании:

* Отчета о результатах проведения внутренней проверки;
* [Перечня персональных данных, подлежащих защите](file:///C:\Users\G-.-Host.G--Host\Desktop\Нотариат\Приложение%206%20Перечень%20персональных%20данных,%20подлежащих%20защите.doc);
* [Акта классификации информационной системы персональных данных](file:///C:\Users\G-.-Host.G--Host\Desktop\Нотариат\Приложение%209%20Акт%20классификации%20информационной%20системы%20персональных%20данных.doc);
* [Модели угроз безопасности персональных данных](file:///C:\Users\G-.-Host.G--Host\Desktop\Нотариат\Приложение%2011%20Модель%20угроз%20безопасности%20персональных%20данных.doc);
* [Положения о разграничении прав доступа к обрабатываемым персональным данным](file:///C:\Users\G-.-Host.G--Host\Desktop\Нотариат\Приложение%2010%20Положение%20о%20разграничении%20прав%20доступа%20к%20обрабатываемым%20персональным%20данным.doc);
* Руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн . На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз и Отчета о результатах проведения внутренней проверке, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

1. **Рекомендации по выбору программно-аппаратных СЗИ**

Выбор программно-аппаратных средств защиты информации для построения СиЗИ

ИСПДн. рекомендуется базировать на следующих принципах:

|  |  |  |
| --- | --- | --- |
|  | **Легитимность** | Программно-аппаратные СЗИ должны быть сертифицированы в системе ФСТЭК и ФСБ России; |
|  | **Необходимость** | СиЗИ ИСПДн. должна быть адекватна угрозам информационной безопасности в части эффективного противодействия существующим и потенциально возможным угрозам информационной безопасности ПДн. |
|  | **Достаточность** | СиЗИ ИСПДн. не должна обладать избыточностью в части своих защитных функций |
|  | **Совместимость** | Выбор СЗИ, необходимо проводить с учетом их возможного взаимодействия с остальными СЗИ ИСПДн., и иными программно-аппаратными компонентами ИСПДн. |
|  | **Стоимость** | Современные условия позволяют Оператору путем самостоятельного поиска, либо путем проведения аукциона определить оптимальную для себя стоимость СЗИ |

Несоблюдение данных принципов может привести к значительным негативным последствиям, в том числе:

* санкциям со стороны контролирующих органов;
* невозможности проведения аттестационных испытаний ИСПДн.;
* снижению реального уровня защищенности ПДн.;
* снижению функциональных возможностей ИСПДн.;
* возникновению дополнительных ошибок и сбоев в работе ИСПДн. (нарушению защитных свойств ПДн.: блокировка, нарушение целостности , уничтожение и т.д.);

**5.Краткий обзор программно-аппаратных средств защиты информации , применимых для создания ИСПДн. в защищенном исполнении**

* 1. **Уровень АРМ: Программно-аппаратные СЗИ разграничения доступа**
     1. **Решения корпорации Microsoft**

|  |  |
| --- | --- |
| **Наименование:** | **Microsoft Windows XP Professional** |
| windows-xp box.jpg  ***Реализация:*** Программная | ***Назначение:***  – клиентская многозадачная и многопользовательская операционная система со встроенной поддержкой одноранговых и клиент-серверных сетей и стека протоколов TCP/IP и IPX/SPX. Позволяет обеспечить взаимодействие с сетями Novell, UNIX и AppleTalk. В состав ОС Microsoft Windows XP Professional включен сервер IIS, предоставляющий платформу для размещения веб-узлов в сетях интранет.   ***Преимущества:*** более высокий уровень безопасности, включая возможность шифрования файлов и папок с целью защиты корпоративной информации;  поддержка мобильных устройств для обеспечения возможности работать автономно или подключаться к компьютеру в удаленном режиме;  встроенная поддержка высокопроизводительных многопроцессорных систем;  возможность работы с серверами Microsoft Windows Server и системами управления предприятиями;   эффективное взаимодействие с другими пользователями по всему миру благодаря возможностям многоязычной поддержки. |
| ***Область применения:***  ИСПДн. Класса К2 - К3 | ***Сертификат соответствия: ФСТЭК России №844/2, №844/3 ОУД 1 (усиленный)*** |

* + 1. **Решения компании ЗАО «НПП «Информационные технологии в бизнесе»**

|  |  |
| --- | --- |
| **Наименование:** | **Панцирь-К** |
| ***Реализация:***   * Программная; * Програмно-аппаратная; | ***Назначение:***  Система предназначена для защиты информации, обрабатываемой на автономном компьютере, либо на компьютерах в составе корпоративной сети. КСЗИ служит для эффективного противодействия, как известным, так и потенциально возможным атакам на защищаемые ресурсы, что обеспечивается устранением архитектурных недостатков защиты современных ОС.  ***Приемущества:***  КСЗИ может применяться для защиты, как от внешних, так и от внутренних ИТ-угроз, обеспечивая эффективное противодействия атакам и со стороны хакеров, и со стороны инсайдеров (санкционированных пользователей, допущенных к обработке информации на защищаемом вычислительном средстве).       КСЗИ также может использоваться для эффективного противодействия вирусным атакам и шпионским программам. |
| ***Область применения:***  ИСПДн. Класса К2 - К3 | ***Сертификат соответствия: ФСТЭК России №1973 - СВТ 5 , НДВ 4*** |

* + 1. **Решения компании ЗАО "НПЦ "Модуль"**

|  |  |
| --- | --- |
| **Наименование:** | **Страж NT версия 3.0** |
| C:\Users\G-.-Host\Downloads\рисунок.jpg  ***Реализация:***   * Программная; * Програмно-аппаратная; | ***Назначение:***  Система защиты информации от несанкционированного доступа  ***Функциональные возможности:***  1.Подсистема контроля устройств Возможность контроля устройств, подключенных к компьютеру путём задания дескрипторов безопасности для групп однотипных устройств. 2.Подсистема преобразования информации на отчуждаемых носителях 3. Защита съемных носителей (дискет и флэш-накопителей) путем прозрачного преобразования всей информации, записываемой на носитель.  4. Подсистема создания и применения шаблонов настроек 5. Поддержка в качестве персональных идентификаторов ГМД, USB-ключей и флэш-накопителей 6. Подсистема учёта носителей информации 7. Подсистема регистрации событий СЗИ 8. Подсистема маркировки и учёта документов, выдаваемых на печать 9. Подсистема управления пользователями 10.Подсистема настройки системы защиты       КСЗИ также может использоваться для эффективного противодействия вирусным атакам и шпионским программам. |
| ***Область применения:***  ИСПДн. Класса К1 - К3 | ***Сертификат соответствия: ФСТЭК России №2145 - СВТ 3 , НДВ 2*** |

* + 1. **Решение компании ООО «Код Безопасности»**

|  |  |
| --- | --- |
| **Наименование:** | **Secret Net (версия 6.0) автономный вариант** |
| C:\Users\G-.-Host\Downloads\file0029.jpg  ***Реализация:***   * Программная; * Програмно-аппаратная; | ***Назначение:***  Система защиты информации  ***Функциональные возможности:***  1.Разграничение доступа.  2.Усиленная идентификация и аутентификация пользователей СЗИ совместно с ОС Windows обеспечивает идентификацию и аутентификацию пользователя с помощью программно-аппаратных средств при его входе в систему.  3.Управление доступом пользователей к конфиденциальным данным  4. Разграничение доступа к устройствам  5. Защита от загрузки с внешних носителей; 6.Защищенная программная среда;  7.Контроль целостности;  8. Контроль аппаратной конфигурации компьютера.  9. Функциональный самоконтроль подсистем  10. Шифрование файлов  11. Контроль печати конфиденциальной информации.  12. Гарантированное уничтожение данных  13. Регистрация событий  14. Импорт и экспорт параметров  шпионским программам. |
| ***Область применения:***  ИСПДн. Класса К1 - К3 | ***Сертификат соответствия: ФСТЭК России №1957 - СВТ 4 , НДВ 4*** |

* + 1. **Решения компании ЗАО "Аладдин Р.Д"**

|  |  |
| --- | --- |
| **Наименование:** | **Secret Disk (версия 4)** |
| рисунок.jpg  ***Реализация:***   * Программная; * Програмно-аппаратная; | ***Назначение:***  Cистема защиты конфиденциальной информации  ***Функциональные возможности:***  1.Шифрование системного раздела, разделов на жестких дисках, томов на динамических дисках, виртуальных дисков и съемных носителей;  2. Аутентификация пользователя по USB-ключу eToken или смарт-карте для загрузки ОС и для доступа к зашифрованным данным;  3. Запрет доступа по сети к зашифрованным данным для всех пользователей, включая системного администратора;  4. Восстановление доступа к данным в случае утери USB-ключа;  5.Защита данных от сбоев во время операций шифрования, включая перебои электропитания;  6. Динамическое распределение скорости шифрования. |
| ***Область применения:***  ИСПДн. Класса К2 - К3 | ***Сертификат соответствия:***  ***ФСТЭК России №1742/1 – ОУД 1 (усиленный)*** |

Обзор программно-аппаратных СЗИ применимых для построения СиЗИ ИСПДн. приведен в **приложении 34.**

* 1. **Уровень АРМ: Антивирусная защита**
     1. **Решения компании ООО «Доктор Веб»**

|  |  |
| --- | --- |
| **Наименование:** | **Dr.Web для Windows (версия 5.0)** |
| C:\Users\G-.-Host\Desktop\рисунок3.jpg  ***Реализация:***   * Программная; | ***Назначение:***  Антивирусная защита информации  ***Функциональные возможности:***    1. Детектирование и нейтрализация вирусов и вредоносных объектов на жестких дисках, сменных носителях и в оперативной памяти.  2. Перехват «на лету» всех обращений к файлам на дисках, CD/DVD/ Blu-ray и т.д.  3. Защита от вирусов, использующих rootkit-технологии  4. Обнаружение и нейтрализация вирусов, существующих в оперативной памяти  и никогда не встречающиеся в виде отдельных файлов 5. Защита от неизвестных угроз при помощи технологии несигнатурного поиска  6. Определение вирусов в архивах  7. Проверка входящей и исходящей корреспонденции на вирусы  8. Защита от массовых рассылок с компьютера сообщений почтовыми червями  9. Защита от НСД извне, предотвращение утечек важных данных по сети, блокировка подозрительных соединений на уровне пакетов и приложений  10. Сканирования по требованию, индивидуальные графики проверок ПК  12. Автоматические уведомления об обнаруженных инфицированных,  неизлечимых или подозрительных объектах  13. Централизованное управление настройками всех компонентов  . |
| ***Область применения:***  ИСПДн. Класса К1 - К3 | ***Сертификаты соответствия:***  ***ФСТЭК России №2012 – НДВ 2, ТУ ФСБ СФ019/1417 - класс B1*** |

* + 1. **Решения компании ЗАО «Лаборатория Касперского»**

|  |  |
| --- | --- |
| **Наименование:** | **Антивирус Касперского**  **для Windows Workstation (версия 6.0)** |
| C:\Users\G-.-Host\Desktop\рисунок4.jpg  ***Реализация:***   * Программная; | ***Назначение:***  Антивирусная защита информации  ***Функциональные возможности:***      1. Защита от вирусов и шпионских программ в режиме реального времени  2. Проверка операционной системы и приложений на наличие уязвимостей  3. Аварийное восстановление для лечения и восстановления системы после заражения  4. Автоматическая проверка и обновление по расписанию |
| ***Область применения:***  ИСПДн. Класса К1 - К3 | ***Сертификат соответствия:***  ***ФСТЭК России №1384 – НДВ3, ТУ*** |

* + 1. **Решения компании ООО «ВирусБлокАда»**

|  |  |
| --- | --- |
| **Наименование:** | **VBA 32 (версия 3.12)** |
| ***Реализация:***   * Программная; | ***Назначение:***  Антивирусная защита информации  ***Функциональные возможности:***      1. Проверка архивов, созданных наиболее употребляемыми архиваторами: RAR, ZIP, ARJ, TAR, GZIP, BZIP2, MS CAB.  2. Обработка (включая обезвреживание) сообщений в почтовых базах Microsoft Outlook Express 4 и 5, Microsoft Outlook, "The Bat!".  3. Использование технологии "Deltapatching" для многократного снижения объема информации, скачиваемой из Интернета при обновлении.  4.Эвристический анализатор и технология распознавания вирусов "MalwareScopeТМ".  5. Технология SOTeCheck, включающейся в работу при малой активности компьютера, для дальнейшего ускорения антивирусной обработки.  6. Эмулятор процессора с динамической трансляцией кода, эффективно обрабатывающий полиморфные, упакованные и зашифрованные вирусы, используется в универсальном распаковщике исполняемых файлов, обработанных различными программами защиты кода от исследования и программами-упаковщиками.  7. Контроль целостности и автоматическая подмена поврежденных модулей позволяет повысить надежность работы антивируса. |
| ***Область применения:***  ИСПДн. Класса К1 - К3 | ***Сертификат соответствия:***  ***ФСТЭК России №1671 – НДВ4, ТУ*** |

* + 1. **Решения компании Symantec**

|  |  |
| --- | --- |
| **Наименование:** | **Symantec AntiVirus Enterprise Edition (версия 10)** |
| C:\Users\G-.-Host.G--Host\Desktop\рисунок4.jpg  ***Реализация:***   * Программная; | ***Назначение:***  Антивирусная защита информации  ***Функциональные возможности:***      1.Общекорпоративная защита от вирусов и мониторинг через единую консоль управления  2. Встроенные графические отчеты на базе Web  3. Защита от шпионского и рекламного ПО  4. Отображение степени влияния шпионского ПО на основе матрицы рисков Symantec (Risk Impact Matrix)  5. Средства защиты от вмешательства Symantec предотвращают НСД к антивирусу и атаки на него, защищая пользователей от тех вирусов, которые пытаются заблокировать меры безопасности |
| ***Область применения:***  ИСПДн. Класса К2 - К3 | ***Сертификат соответствия:***  ***ФСТЭК России №1671 – НДВ4, ТУ*** |

* + 1. **Решения компании ЗАО «ИСЕТ»**

|  |  |
| --- | --- |
| **Наименование:** | **Eset NOD32 Platinum Pack (версия 4.0)** |
| C:\Users\G-.-Host.G--Host\Desktop\рисунок7.jpg  ***Реализация:***   * Программная; | ***Назначение:***  Антивирусная защита информации  ***Функциональные возможности:***    1.Проактивная защита и точное обнаружение угроз. 2.Технология ThreatSense®. Ядро программы обеспечивает проактивное обнаружение всех типов угроз и лечение зараженных файлов (в том числе, в архивах) благодаря широкому применению интеллектуальных технологий, сочетанию эвристических методов и традиционного сигнатурного детектирования.  3. Host Intrusion Prevention System (HIPS). Система защиты от попыток внешнего воздействия, способных негативно повлиять на безопасность компьютера. Для мониторинга процессов, файлов и ключей реестра HIPS используется сочетание технологий поведенческого анализа с возможностями сетевого фильтра, что позволяет эффективно детектировать, блокировать и предотвращать подобные попытки вторжения. |
| ***Область применения:***  ИСПДн. Класса К1 - К3 | ***Сертификат соответствия:***  ***ФСТЭК России №1914 – НДВ 4; ТУ*** |

* 1. **Уровень внутрисетевого взаимодействия: Программно-аппаратные СЗИ разграничения доступа**
     1. **Решения корпорации Microsoft**

|  |  |
| --- | --- |
| **Наименование:** | **Microsoft Windows Server 2008 Standart Edition** |
| C:\Users\G-.-Host.G--Host\Desktop\рисунок12.jpg  ***Реализация:***   * Программная; | ***Назначение:***  Серверная операционная система.   ***Преимущества*:**  Новые средства управления и усовершенствованные функции безопасности обеспечивают полный контроль над серверами и расширенную защиту.  ***Виртуализация***  Благодаря технологии Hyper-V, которая в Windows Center 2008 отвечает за виртуализацию, на единственном физическом сервере можно совместить несколько разных серверов со специализированными приложениями.  ***Веб-платформа***  Службы IIS 7.0 являются главным усовершенствованием существующего веб-сервера Windows и играют главную роль в интеграции технологий веб-платформ. Они помогают разработчикам и администраторам поддерживать максимальный контроль над интерфейсами сети и Интернета при помощи ключевых функций. |
| ***Область применения:***  ИСПДн. Класса К3 | ***Сертификат соответствия: ФСТЭК России №1928 – СВТ 5*** |

* 1. **Уровень межсетевого взаимодействия: Межсетевые экраны, VPN** 
     1. **Решения компании ООО «Код Безопасности»**

|  |  |
| --- | --- |
| **Наименование:** | **АПКШ Континент (версия 3.5)** |
| C:\Users\G-.-Host.G--Host\Desktop\рисунок8.jpg  ***Реализация:***   * Программно-аппаратная; | ***Назначение:***  Программно-аппаратный комплекс шифрования позволяющий обеспечить защиту корпоративных сетей от атак со стороны открытых сетей передачи данных, конфиденциальность информации, передаваемой через открытые сети (путем  организации VPN), организовать безопасный доступ пользователей к ресурсам сетей  общего пользования и защищенное соединение локальных сетей организации с использованием сети общего пользования.  ***Функциональные возможности:***    1. Объединение через Интернет локальных сетей предприятия в единую сеть VPN;  2. Подключение удаленных и мобильных пользователей к VPN по защищенному каналу;  3. Разделение доступа между информационными подсистемами организации;  4. Организация защищенного взаимодействия со сторонними организациями;  5. Безопасное удаленное управление маршрутизаторами. |
| ***Область применения:***  ИСПДн. Класса К1-К3 | ***Сертификаты соответствия:***  ***ФСТЭК России №1905 - МЭ 3 НДВ 3***  ***ФСБ России №СФ/525-1352 - МЭ 4***  ***ФСБ России №СФ/124-1396 - СЗИ КС2*** |

* + 1. **Решения компании Cisco Systems**

|  |  |
| --- | --- |
| **Наименование:** | **Cisco ASA 5510** |
| C:\Users\G-.-Host.G--Host\Desktop\рисунок9.jpg  ***Реализация:***   * Программно-аппаратная; | ***Назначение:***  Многофункциональный программно-аппаратный комплекс, предназначенный для разграничения доступа к сетевым ресурсам, защиты от атак, защиты  взаимодействия с удаленными территориями, блокирования вирусов,  червей, шпионского ПО и других вредоносных программ, спама и атак типа «фишинг».  ***Функциональные возможности:***    1. Поддержка VLAN  2. Поддержка отказоустойчивых конфигураций (Active/Standby и Active/Active)  3. Поддержка механизмов управления сигналами тревоги.  4. Поддержка OSPF,PIM,Ipv6,QoS  5. Поддержка виртуальных и прозрачных МСЭ  6. Контроль протоколов и приложений (Web,e-mail,FTP голос и мультимедиа,СУБД, операционных систем GTR/GPRS,ISQ,P2P и т.п)  7. Защита от атак «переполнение буфера», нарушения RFC,аномалий,подмены адреса  8. Организация SSL и IPSec VPN  9. Отражение вирусов, червей и вредоносных программ в протоколах HTTP,FTP,SMTP и POP3 |
| ***Область применения:***  ИСПДн. Класса К2-К3 | ***Сертификаты соответствия:***  ***ФСТЭК России №1263/1 - МЭ 4; ТУ*** |

* + 1. **Решения Stonesoft Corporation**

|  |  |
| --- | --- |
| **Наименование:** | **StoneGate Firewall/VPN** |
| C:\Users\G-.-Host.G--Host\Desktop\рисунок17.jpgC:\Users\G-.-Host.G--Host\Desktop\рисунок15.jpg  ***Реализация:***   * Программно-аппаратная; | ***Назначение:***  Линейка программных и программно-аппаратных межсетевых экранов  с возможностью построения отказоустойчивых VPN.    ***Функциональные возможности:***   1. Фильтрация сетевого трафика с возможностью контроля состояния (statefull inspection);  2. SSL Inspection - встроенные возможности по дешифрованию SSL-трафика с целью проверки на наличие вредоносного кода;  3. Web-фильтрация - позволяет закрыть доступ сотрудников организации к вредоносным и нежелательным сайтам;  4. Deep Packet Inspection - технология глубокого анализа трафика на прикладном уровне;  5. Кластеризация- все устройства имеют встроенные возможности кластеризации и балансировки нагрузок между несколькими FW/VPN-устройствами;  6. Защита от DoS/DDoS - позволяет блокировать наиболее распространенные типы DoS-атак (таких как SYN flood, UDP flood и другие);  7. Встроенное хранилище IPS-сигнатур позволяет FW/VPN выполнять часть функций устройства IPS;  8. Обеспечение QoS(Quality of Service) - встроенные возможности по управлению полосой пропускания позволяют распределить объемы полосы среди всех бизнес-приложений, исходя из их приоритета; |
| ***Область применения:***  ИСПДн. Класса К1-К3 | ***Сертификаты соответствия:***  ***ФСТЭК России №2157 - МЭ 2; НДВ 4; ТУ*** |

* + 1. **Решения компании Entensys**

|  |  |
| --- | --- |
| **Наименование:** | **UserGate Proxy & Firewall (версия 5.2.F)** |
| C:\Users\G-.-Host.G--Host\Desktop\рисунок10.jpg  ***Реализация:***   * Программная; | ***Назначение:***  Комплексное решение для организации общего доступа в Интернет из  локальной сети, учета трафика и защиты корпоративной сети от внешних угроз.  ***Функциональные возможности:***    1. Межсетевой экран  2. Встроенная антивирусная защита  3. Усиленные механизмы аутентификации  4. Расширенный драйвер NAT  5. Поддержка VPN-соединений  6. Организация доступа в Интернет  7. Фильтрация веб-сайтов  8. Ограничение трафика  9. Регулирование скорости доступа  10. Учет трафика  11. Модуль веб-статистики  12. Биллинговая система  13. Поддержка различных протоколов  14. Управление шириной канала  15. Кэширование трафика  16. Поддержка IP-телефонии  17. Маршрутизация  18. DHCP-сервер  19. Публикация ресурса  20. Аудит и подробная статистика действий  21. пользователей и администраторов  22. Защищенный доступа в Интернет  23. Контроль приложений |
| ***Область применения:***  ИСПДн. Класса К1-К3 | ***Сертификаты соответствия:***  ***ФСТЭК России №2076 - ОУД 2; МЭ4 ; НДВ 4*** |

* + 1. **Решения компании ОАО «Инфотекс»**

|  |  |
| --- | --- |
| **Наименование:** | **ViPNet CUSTOM (версия 3.0)** |
| C:\Users\G-.-Host.G--Host\Desktop\рисунок11.jpg  ***Реализация:***   * Программная; | ***Назначение:***  Предназначен для объединения в единую защищенную виртуальную сеть  произвольного числа рабочих станций, мобильных пользователей и локальных сетей.  ***Функциональные возможности:***     1. Создание защищенной, доверенной среды передачи конфиденциальной информации с использованием публичных и выделенных каналов связи (Интернет, телефонные и телеграфные линии связи и т.п.), путем организации виртуальной частной сети ( VPN ). 2. Развертывание инфраструктуры открытых ключей ( PKI ) и организации Удостоверяющего Центра с целью интеграции механизмов электронно-цифровой подписи в прикладное программное обеспечение заказчика (системы документооборота и делопроизводства, электронную почту, банковское программное обеспечение, электронные торговые площадки и витрины). Поддерживается возможность взаимодействия с программным обеспечением PKI других отечественных производителей, например, ЗАО «Сигнал-КОМ» и ООО «Крипто-Про». |
| ***Область применения:***  ИСПДн. Класса К1-К3 | ***Сертификаты соответствия:***  ***ФСТЭК России №1549 - ОУД 4+ ; МЭ 3; НДВ 3*** |

|  |  |
| --- | --- |
| **Наименование:** | **ViPNet Office Firewall** |
| ***Реализация:***   * Программная; | ***Назначение:***  Программный межсетевой экран, обеспечивающий защиту компьютеров локальной сети от несанкционированного доступа при работе по протоколу IP с другими локальными или глобальными сетями, например Интернет. Программное обеспечение (ПО) ViPNet Office Firewall устанавливается на сервер–шлюз и контролирует весь IP-трафик, проходящий через этот шлюз в/из локальной сети.  ***Функциональные возможности:***   1. Защита локальной сети от атак из сети Интернет 2. Управление доступом к Интернет-ресурсам из локальной сети 3. Защита нескольких локальных сетей и ДМЗ |
| ***Область применения:***  ИСПДн. Класса К1-К3 | ***Сертификаты соответствия:***  ***ФСТЭК России №546/1/1 – МЭ 3; НДВ 3***  ***ФСБ России №СФ/115-1286 - МЭ 4*** |

1. **Сравнительная технико-экономическая оценка сертифицированных программно-технических средств, которые могут быть использованы при создании СиЗИ ИСПДн.**

В соответствии со структурой схемой системы обеспечения безопасности информации и с учетом функциональных возможностей сертифицированных программно-технических средств, которые могут быть использованы при создании СиЗИ ИСПДн., сравнительная технико-экономическая оценка будет проведена с учетом следующих уровней требующих защиты:

* ***Уровень АРМ: Программно-аппаратные СЗИ разграничения доступа***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Разработчик:** | **Microsoft** | **ЗАО «НПП «Информационные технологии в бизнесе»** | **ЗАО "НПЦ "Модуль"** | **ЗАО "Аладдин Р.Д"** | **ООО «Код Безопасности»** |
| **Контактная информация:** | http://www.microsoft.com/ru/ru/ | http://www.npp-itb.spb.ru/ | <http://www.guardnt.ru/> | http://www.aladdin.ru/ | http://www.securitycode.ru/ |
| 121614, Москва Крылатская улица, д. 17 | 194044, Санкт-Петербург, пр. Большой Сампсониевский, д.32, | 105318, г. Москва, Измайловское шоссе, дом 20, стр. 1 | 129226, Москва, ул. Докукина, д. 16, корп.1 | 127018, Москва, ул. Образцова, 38 |
| (495)916-7171 | (812) 324-27-71 | (495) 411-9912 | (495) 223-0001 | (495) 980–2345 |
| **Полное наименование:** | **Microsoft Windows XP (SP3) Professional** | **Панцирь К** | **Страж NT версия 3.0** | **Secret Disk 4** | **Secret Net 6.0 (автономный вариант)** |
| **Наличие сертификатов:** | ФСТЭК России №844/2, №844/3  (истекает 3.12.2011) ОУД 1 (усиленный) | ФСТЭК России №1973 СВТ 5 НДВ 4 | ФСТЭК России №2145  СВТ 3 НДВ 2 | ФСТЭК Россси №1742/1 (истекает 06.05.2013) ОУД 1 (усиленный) АС класс 1Г ИСПДн. класс 2 | ФСТЭК России №1957 СВТ 4 НДВ 4 АС класс 1Г ИСПДн. класс 1 |
| **Область применения:** | **ИСПДн K3** | **ИСПДн К2-K3** | **ИСПДн К1-K3** | **ИСПДн К2-K3** | **ИСПДн К1-K3** |
| **Реализация:** | *Программная* | *Программная* | *Программно-аппаратная* | *Программно-аппаратная* | *Программно-аппаратная* |
| **Предназначение средства (область применения), краткая характеристика параметров**  **Предназначение средства (область применения), краткая характеристика параметров** | Операционная система | Комплексная система защиты информации *Функциональные возможности:*  1. Разграничение доступа к локальным и разделенным в сети ресурсам – к файловым объектам, к объектам реестра ОС, к внешних накопителям, к принтерам, к сетевым хостам и др.; 2. Включение в разграничительную политику субъекта "процесс", как самостоятельного субъекта доступа к ресурсам, принципиально расширяющее функциональные возможности защиты и противодействующий атакам на расширение привилегий;  3. Управление подключением устройств; 4. Обеспечение замкнутости программной среды; 5. Контроль целостности файловых объектов (программ и данных); 6. Контроль корректности функционирования СЗИ;  7. Возможность подключать аппаратные средства ввода парольных данных (eToken и др.); 8. Контроль корректности идентификации субъекта доступа к ресурсам (контроль олицетворения);  9. Противодействие ошибкам и закладкам в системном и в прикладном ПО; 10. Шифрование данных, реализующий ключевую политику, обеспечивающую невозможность несанкционированно раскрыть похищенную информацию (в том числе и собственно пользователем, ее обрабатывающим - инсайдером), даже при наличии у похитителя ключа шифрования. | Система защиты информации от несанкционированного доступа *Функциональные возможности:* 1.Подсистема контроля устройств Возможность контроля устройств, подключенных к компьютеру путём задания дескрипторов безопасности для групп однотипных устройств. 2.Подсистема преобразования информации на отчуждаемых носителях 3. Защита съемных носителей (дискет и флэш-накопителей) путем прозрачного преобразования всей информации, записываемой на носитель.  4. Подсистема создания и применения шаблонов настроек 5. Поддержка в качестве персональных идентификаторов ГМД, USB-ключей и флэш-накопителей 6. Подсистема учёта носителей информации 7. Подсистема регистрации событий СЗИ 8. Подсистема маркировки и учёта документов, выдаваемых на печать 9. Подсистема управления пользователями 10.Подсистема настройки системы защиты | Cистема защиты конфиденциальной информации Функциональные возможности: 1.Шифрование системного раздела, разделов на жестких дисках, томов на динамических дисках, виртуальных дисков и съемных носителей;  2. Аутентификация пользователя по USB-ключу eToken или смарт-карте для загрузки ОС и для доступа к зашифрованным данным;  3. Запрет доступа по сети к зашифрованным данным для всех пользователей, включая системного администратора;  4. Восстановление доступа к данным в случае утери USB-ключа;  5.Защита данных от сбоев во время операций шифрования, включая перебои электропитания;  6. Динамическое распределение скорости шифрования. | Система защиты информации Функциональные возможности: 1.Разграничение доступа. 2.Усиленная идентификация и аутентификация пользователей СЗИ совместно с ОС Windows обеспечивает идентификацию и аутентификацию пользователя с помощью программно-аппаратных средств при его входе в систему. В качестве устройств для ввода в нее идентификационных признаков могут быть использованы: ( iButton;eToken Pro).  3.Управление доступом пользователей к конфиденциальным данным  4. Разграничение доступа к устройствам  5. Защита от загрузки с внешних носителей; 6.Защищенная программная среда;  7.Контроль целостности;  8. Контроль аппаратной конфигурации компьютера.  9. Функциональный самоконтроль подсистем  10. Шифрование файлов  11. Контроль печати конфиденциальной информации.  12. Гарантированное уничтожение данных  13. Регистрация событий  14. Импорт и экспорт параметров |
| **Поддерживаемые ОС:** | **MS Windows XP (SP3) Professional** | **MS Windows 2000 - Vista** | **MS Windows**  **Vista - 7** | **Microsoft Windows 2000, XP, Vista, Windows 7** | **MS Windows**  **Vista - 7** |
| **Ориентировочная стоимость** | **2500** | **http://www.npp-itb.spb.ru/prices/index.shtml** | **7 500** | **4720** | **6400** |

***уровень АРМ: антивирусы***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Разработчик:** | **ООО «Доктор Веб»** | **Symantec** | **ЗАО «Лаборатория Касперского»** | **ООО «ВирусБлокАда»** | **ЗАО «ИСЕТ»** |
|
| **Контактная информация:** | <http://www.drweb.com/> | [http://www.symantec.com](http://www.symantec.com/) | <http://www.kaspersky.ru/> | <http://www.vba.com.by/> | <http://www.esetnod32.ru/> |
| 125124, Москва, 3-я улица Ямского поля, вл.2, корп.12А | 123317, Россия, Москва, Краснопресненская набережная, 18 | 123060, Москва, 1-й Волоколамский пр-д, д. 10, стр. 1 | 127106 г. Москва, ул. Гостиничная, д. 10, корп. 5 | 115114, Москва, Дербеневская набережная, д.7, стр. 14 |
| (495) 789-45-87 | (495) 662-8300 | (495) 797-8700 | (495) 221-21-07 | (495) 797-26-94 |
| **Полное наименование:** | **Dr.Web для Windows версии 5.0** | **Symantec AntiVirus Enterprise Edition» v. 10.1** | **Антивирус Касперского 6.0 для Windows Workstations** | **VBA32 3.12** | **Eset NOD32 Platinum Pack 4.0** |
| **Наличие сертификатов:** | ФСТЭК России №2012 НДВ2 ТУ ФСБ СФ019/1417 класс B1 | ФСТЭК России №1545 ТУ ИСПДн. класс 2 | ФСТЭК России №1384 НДВ3 ТУ | ФСТЭК России №1671 НДВ4 ТУ ИСПДн. класс 1 | ФСТЭК России №1914 НДВ4 ТУ АС 1Г ИСПДн. класс 1 |
| **Область применения:** | **ИСПДн К1-K3** | **ИСПДн К2-К3** | **ИСПДн К1-K3** | **ИСПДн К1-K3** | **ИСПДн К1-K3** |
| **Предназначение средства (область применения), краткая характеристика параметров**  **Предназначение средства (область применения), краткая характеристика параметров**  **Предназначение средства (область применения), краткая характеристика параметров** | Программное изделие «Антивирус Dr. Web® версии 5.0 для Windows» *Функциональные возможности:* 1. Детектирование и нейтрализация вирусов и вредоносных объектов на жестких дисках, сменных носителях и в оперативной памяти. 2. Перехват «на лету» всех обращений к файлам на дисках, дискетах, CD/DVD/ Blu-ray дисководах, Flash- и смарт-картах 3. Защита от вирусов, использующих rootkit-технологии 4. Обнаружение и нейтрализация вирусов, существующих в оперативной памяти и никогда не встречающиеся в виде отдельных файлов 5. Защита от неизвестных угроз при помощи технологии несигнатурного поиска Origins Tracing™ и интеллектуального эвристического анализатора Dr.Web 6. Определение вирусов в архивах любой степени вложенности и в упакованных объектах 7. Проверка входящей и исходящей корреспонденции на вирусы по протоколам SMTP/POP3/NNTP/IMAP 8. Защита от массовых рассылок с компьютера сообщений почтовыми червями 9. Защита от НСД извне, предотвращение утечек важных данных по сети, блокировка подозрительных соединений на уровне пакетов и приложений 10. Сканирования по требованию, индивидуальные графики проверок ПК 11. Автоматический прием обновлений вирусной базы Dr.Web с любой нужной периодичностью 12. Автоматические уведомления об обнаруженных инфицированных, неизлечимых или подозрительных объектах 13. Централизованное управление настройками всех компонентов 14. Прозрачность работы – подробные отчеты о работе каждого модуля | Программное обеспечение система антивирусной защиты *Функциональные возможности:* 1.Общекорпоративная защита от вирусов и мониторинг через единую консоль управления 2. Встроенные графические отчеты на базе Web 3. Защита от шпионского и рекламного ПО 4. Отображение степени влияния шпионского ПО на основе матрицы рисков Symantec (Risk Impact Matrix) 5. Средства защиты от вмешательства Symantec предотвращают НСД к антивирусу и атаки на него, защищая пользователей от тех вирусов, которые пытаются заблокировать меры безопасности | ПО «Антивирус Касперского 6.0 для Windows Workstations» *Функциональные возможности:*  1. Защита от вирусов и шпионских программ в режиме реального времени 2. Проверка операционной системы и приложений на наличие уязвимостей 3. Тонкая настройка компьютера для повышения его производительности и уровня защиты 4. Аварийное восстановление для лечения и восстановления системы после заражения 5. Автоматическая проверка и обновление по расписанию | Программный комплекс антивирусной защиты. *Функциональные возможности:*  1. Проверка архивов, созданных наиболее употребляемыми архиваторами: RAR, ZIP, ARJ, TAR, GZIP, BZIP2, MS CAB. 2. Обработка (включая обезвреживание) сообщений в почтовых базах Microsoft Outlook Express 4 и 5, Microsoft Outlook, "The Bat!". 3. Использование технологии "Deltapatching" для многократного снижения объема информации, скачиваемой из Интернета при обновлении. 4.Эвристический анализатор и технология распознавания вирусов "MalwareScopeТМ".  5. Технология SOTeCheck, включающейся в работу при малой активности компьютера, для дальнейшего ускорения антивирусной обработки. 6. Эмулятор процессора с динамической трансляцией кода, эффективно обрабатывающий полиморфные, упакованные и зашифрованные вирусы, используется в универсальном распаковщике исполняемых файлов, обработанных различными программами защиты кода от исследования и программами-упаковщиками. 7. Контроль целостности и автоматическая подмена поврежденных модулей позволяет повысить надежность работы антивируса. | Пакет программ. *Функциональные возможности:* 1.Проактивная защита и точное обнаружение угроз. 2.Технология ThreatSense®. Ядро программы обеспечивает проактивное обнаружение всех типов угроз и лечение зараженных файлов (в том числе, в архивах) благодаря широкому применению интеллектуальных технологий, сочетанию эвристических методов и традиционного сигнатурного детектирования. 3. Host Intrusion Prevention System (HIPS). Система защиты от попыток внешнего воздействия, способных негативно повлиять на безопасность компьютера. Для мониторинга процессов, файлов и ключей реестра HIPS используется сочетание технологий поведенческого анализа с возможностями сетевого фильтра, что позволяет эффективно детектировать, блокировать и предотвращать подобные попытки вторжения. |
| **Системные требования:** | Свободное пространство на жестком диске: ~40 МБ. Дополнительно для установки брандмауэра необходимо ~ 8 МБ. Доступ к сети Интернет: для регистрации и получения обновлений. | MS Windows 2000 • 64 МБ ОЗУ • (Microsoft Internet Explorer 5.5 SP2) MS Windows XP Professional • 64 МБ ОЗУ • (Microsoft Internet Explorer 5.5 SP2) MS Windows Server 2003 • 64 МБ ОЗУ • (Microsoft Internet Explorer 5.5 SP2) | *Microsoft Windows XP Professional [32, x64 (Service Pack 2 или выше)*   Аппаратные требования: 1. Процессор с частотой 800 МГц или выше 2. 512 Мб свободной оперативной памяти. *MS Windows Vista Business, Enterprise, Ultimate (x32 и x64), MS Windows 7 Профессиональная, Максимальная (x32 и x64)* |  | 1. Поддерживаемые процессоры: 32-разрядный (x86) и 64-разрядный (x64) Intel®, AMD® 2. Память: 44 MB 3. Объем дискового пространства (загрузка): 28 MB 4. Объем дискового пространства (установка): 35 MB |
| **ориентировочная стоимость, руб** | **900** | **1392,75** | **1200** | **2061,27** | **2500** |

* ***Уровень межсетевого взаимодействия: Межсетевые Экраны***

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Разработчик** | **ООО «Код Безопасности»** | **Stonesoft Corporation** | **Cisco Systems** | **ОАО «Инфотекс»** | | **Entensys** |
|
| **Контактная информация** | <http://www.securitycode.ru/> | <http://www.stonesoft.com/> | <http://www.cisco.com/> | <http://infotecs.ru/> | | <http://www.usergate.ru/> |
| 127018, Москва, ул. Образцова, 38 | [info.emea@stonesoft.com](mailto:info.emea@stonesoft.com) | 115054, Москва, Космодамианская набережная, 52, стр.1 | 127287,Москва, Ст.Петровско-Разумовский пр-д, д.1/23, стр.1 | | 630090, г. Новосибирск, ул. Терешковой, 29 |
| (495) 980–2345 |  | (495) 961-1410 | (495) 737-61-92 | | (383) 330-29-13 |
|
| **Полное наименование** | **АПКШ Континент (версия 3.5)** | **StoneGate Firewall/VPN** | **Cisco ASA 5510** | **ViPNet CUSTOM 3.0** | **ViPNet Office Firewall** | **UserGate Proxy & Firewall 5.2.F** |
| **Наличие сертификатов** | ФСТЭК России №1905 МЭ 3 НДВ 3 АС 1Г ФСБ России №СФ/525-1352 МЭ 4 ФСБ России №СФ/124-1396 СЗИ КС2 | ФСТЭК России № 2157 МЭ 2 НДВ 4 ТУ АС 1Г | ФСТЭК России №1263/1 МЭ 4 ТУ | ФСТЭК России №1549 ОУД 4+ МЭ 3 НДВ 3 АС 1В | ФСТЭК России №546/1/1 МЭ 3 НДВ 3 ФСБ России №СФ/115-1286 МЭ 4 | ФСТЭК России №2076 ОУД 2 МЭ4 НДВ 4 |
| **Область применения** | **ИСПДн К1-K3** | **ИСПДн К1-K3** | **ИСПДн K2-К3** | **ИСПДн K1-К3** | **ИСПДн K1-К3** | **ИСПДн K1-К3** |
| **Реализация** | *Программно-аппаратная* | *Программно-аппаратная* | *Программно-аппаратная* | *Программная* | *Программная* | *Программная* |
| **Предназначение средства (область применения), краткая характеристика параметров**  **Предназначение средства (область применения), краткая характеристика параметров** | Программно-аппаратный комплекс шифрования позволяющий обеспечить защиту корпоративных сетей от атак со стороны открытых сетей передачи данных, конфиденциальность информации, передаваемой через открытые сети (путем организации VPN), организовать безопасный доступ пользователей к ресурсам сетей общего пользования и защищенное соединение локальных сетей организации с использованием сети общего пользования. *Функциональные возможности:* 1. Объединение через Интернет локальных сетей предприятия в единую сеть VPN; 2. Подключение удаленных и мобильных пользователей к VPN по защищенному каналу;  3. Разделение доступа между информационными подсистемами организации;  4. Организация защищенного взаимодействия со сторонними организациями;  5. Безопасное удаленное управление маршрутизаторами. | Линейка программных и программно-аппаратных межсетевых экранов с возможностью построения отказоустойчивых VPN.  *Функциональные возможности:*  1. Фильтрация сетевого трафика с возможностью контроля состояния (statefull inspection); 2. SSL Inspection - встроенные возможности по дешифрованию SSL-трафика с целью проверки на наличие вредоносного кода; 3. Web-фильтрация - позволяет закрыть доступ сотрудников организации к вредоносным и нежелательным сайтам; 4. Deep Packet Inspection - технология глубокого анализа трафика на прикладном уровне; 5. Кластеризация- все устройства имеют встроенные возможности кластеризации и балансировки нагрузок между несколькими FW/VPN-устройствами; 6. Защита от DoS/DDoS - позволяет блокировать наиболее распространенные типы DoS-атак (таких как SYN flood, UDP flood и другие); 7. Встроенное хранилище IPS-сигнатур позволяет FW/VPN выполнять часть функций устройства IPS;  8. нагрузки. | Многофункциональный программно-аппаратный комплекс, предназначенный для разграничения доступа к сетевым ресурсам, защиты от атак, защиты взаимодействия с удаленными территориями, блокирования вирусов, червей, шпионского ПО и других вредоносных программ, спама и атак типа «фишинг». *Функциональные возможности:* 1. Поддержка VLAN  2. Поддержка отказоустойчивых конфигураций (Active/Standby и Active/Active)  3. Поддержка механизмов управления сигналами тревоги Risk Rating,Meta Event Generator  4. Поддержка OSPF,PIM,Ipv6,QoS  5. Поддержка виртуальных и прозрачных МСЭ  6. Контроль протоколов и приложений (Web,e-mail,FTP голос и мультимедиа,СУБД, операционных систем GTR/GPRS,ISQ,P2P и т.п)  7. Защита от атак «переполнение буфера», нарушения RFC,аномалий,подмены адреса  8. Организация SSL и IPSec VPN  9. Отражение вирусов, червей и вредоносных программ в протоколах HTTP,FTP,SMTP и POP3  10. Механизм Syslog to ACL Correlation  11. Контроль до 8 сетевых интерфейсов | ViPNet CUSTOM предназначен для объединения в единую защищенную виртуальную сеть произвольного числа рабочих станций, мобильных пользователей и локальных сетей  *Функциональные возможности:*  1. Создание защищенной, доверенной среды передачи конфиденциальной информации с использованием публичных и выделенных каналов связи (Интернет, телефонные и телеграфные линии связи и т.п.), путем организации виртуальной частной сети ( VPN ). 2. Развертывание инфраструктуры открытых ключей ( PKI ) и организации Удостоверяющего Центра с целью интеграции механизмов электронно-цифровой подписи в прикладное программное обеспечение заказчика (системы документооборота и делопроизводства, электронную почту, | ViPNet [Office Firewall] является программным межсетевым экраном, обеспечивающим надежную защиту компьютеров локальной сети от несанкционированного доступа при работе по протоколу IP с другими локальными или глобальными сетями, например Интернет. Программное обеспечение (ПО) ViPNet [Office Firewall] устанавливается на сервер–шлюз и контролирует весь IP-трафик, проходящий через этот шлюз в/из локальной сети. *Функциональные возможности:* 1. Защита локальной сети от атак из Интернет 2. Управление доступом к Интернет-ресурсам из локальной сети 3. Защита нескольких локальных сетей и ДМЗ | Комплексное решение для организации общего доступа в Интернет из локальной сети, учета трафика и защиты корпоративной сети от внешних угроз. *Функциональные возможности:* 1. Межсетевой экран  2. Встроенная антивирусная защита  3. Усиленные механизмы аутентификации  4. Расширенный драйвер NAT  5. Поддержка VPN-соединений  6. Организация доступа в Интернет  7. Фильтрация веб-сайтов  8. Ограничение трафика  9. Регулирование скорости доступа  10. Учет трафика  11. Модуль веб-статистики  12. Биллинговая система  13. Поддержка различных протоколов  14. Управление шириной канала  15. Кэширование трафика  16. Поддержка IP-телефонии  17. Маршрутизация  18. DHCP-сервер  19. Публикация ресурса  20. Аудит и подробная статистика действий  21. пользователей и администраторов  22. Защищенный доступа в Интернет  23. Контроль приложений |
| **ориентировочная стоимость** |  | **7500** |  |  | **15000** | **3856** |

1. **Типовые варианты системы защиты ПДн. в ИСПДн.**

Сравнительная технико-экономическая оценка отечественных cертифицированных программно-технических средств защиты информации, позволяет предложить следующие варианты построения СиЗИ ИСПДн..

***Уровень защиты АРМ.***

Вариант 1**.**

|  |  |  |  |
| --- | --- | --- | --- |
| Функциональное предназначение | Производитель | Наименование | Стоимость  (руб.) |
| Разграничение и контроль доступа пользователей | Microsoft | Microsoft Windows XP (SP3) Professional | 2500 |
| Антивирусная защита | ЗАО «ИСЕТ» | Eset NOD32 Platinum Pack 4.0 | 2500 |

Ориентировочная стоимость реализации данного варианта, c учётом предоставленных исходных данных, составляет: **5000 руб**.

Вариант 2.

|  |  |  |  |
| --- | --- | --- | --- |
| Функциональное предназначение | Производитель | Наименование | Стоимость  (руб.) |
| Разграничение и контроль доступа пользователей | ЗАО «НПП «Информационные технологии в бизнесе» | Панцирь К | http://www.npp-itb.spb.ru/prices/index.shtml |
| Антивирусная защита | ООО «Доктор Веб» | Dr.Web для Windows версии 5.0 | 900 |

Ориентировочная стоимость реализации данного варианта, c учётом предоставленных исходных данных, составляет: \_\_\_\_\_\_\_\_\_\_\_ руб.

Вариант 3.

|  |  |  |  |
| --- | --- | --- | --- |
| Функциональное предназначение | Производитель | Наименование | Стоимость  (руб.) |
| Разграничение и контроль доступа пользователей | **ЗАО "Аладдин Р.Д"** | **Secret Disk 4** | 4500 |
| Антивирусная защита | **ЗАО «Лаборатория Касперского»** | **Антивирус Касперского 6.0 для Windows Workstations** | 1200 |

Ориентировочная стоимость реализации данного варианта, c учётом предоставленных исходных данных, составляет: **6700 руб**.

* ***Уровень межсетевого взаимодействия: Межсетевые экраны, VPN***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Вариант | Функциональное предназначение | Производитель | Наименование | Стоимость оборудования |
|  | Межсетевой экран, VPN | **Stonesoft Corporation** | **StoneGate Firewall/VPN** | **7500** |
|  | Межсетевой экран, VPN | **ОАО «Инфотекс»** | **ViPNet CUSTOM 3.0** | **46 020,00** |
|  | Межсетевой экран | **ОАО «Инфотекс»** | **ViPNet Office Firewall** | **14500** |
|  | Межсетевой экран | **Check Point** | **EndPoint** |  |

На схемах 1-3 приведены варианты комплексного решения задачи обеспечения безопасности ПДн., обрабатываемых при осуществлении нотариальной деятельности.

Схема 1.

|  |  |
| --- | --- |
| Уровень АРМ: | *Панцирь-К + Антивирус Dr.Web версия 5.0* |
| Уровень Внутрисетевого взаимодействия: | *Панцирь-К + Антивирус Dr.Web версия 5.0* |
| Уровень межсетевого взаимодействия: | *Межсетевой экран StoneGate Firewall/VPN* |

Схема 2.

|  |  |
| --- | --- |
| Уровень АРМ: | *Windows XP Professional SP3 + Антивирус Eset NOD32 Platinum Pack 4.0* |
| Уровень Внутрисетевого взаимодействия: | *Microsoft Windows Server 2008 Standart Edition+ Антивирус Eset NOD32 Platinum Pack 4.0* |
| Уровень межсетевого взаимодействия: | *Межсетевой экран UserGate Proxy & Firewall 5.2.F* |

Схема 3.

|  |  |
| --- | --- |
| Уровень АРМ: | ***Secret Disk 4 + Антивирус Касперского 6.0 для Windows Workstations*** |
| Уровень Внутрисетевого взаимодействия: | *Secret Disk 4 + Антивирус Касперского 6.0 для Windows Workstations* |
| Уровень межсетевого взаимодействия: | *Межсетевой экран ViPNet Office Firewall* |

Схема 4.

|  |  |
| --- | --- |
| Уровень АРМ: | ***Secret Disk 4 + Антивирус Касперского 6.0 для Windows Workstations*** |
| Уровень Внутрисетевого взаимодействия: | *Secret Disk 4 + Антивирус Касперского 6.0 для Windows Workstations+VipNet Client* |
| Уровень межсетевого взаимодействия: | *Межсетевой экран ViPNet Custom* |

1. Технические требования, предъявляемые к рабочим станциям с установленными средствами защиты

Для организации защищенной сети требуются АРМ соответствующие следующим техническим требованиям:

**Для клиентского места защищенной ИСПДн.:**

|  |  |  |
| --- | --- | --- |
|  | **Мин. Требования** | **Рекомендуется** |
| **Процессор:** | 32-разрядный процессор (x86) с тактовой  частотой 1 ГГц; | x86 или x64 с тактовой частотой 1 ГГц |
| **Память:** | 1 ГБ | 2 ГБ |
| **Требуемый объем жесткого диска:** | 40 Гб с 16 Гб свободного дискового пространства | 40 Гб с 16 Гб свободного дискового пространства |
| **Видеокарта** | Поддержка интерфейса DirectX 9, не менее 128 МБ видеопамяти | Поддержка интерфейса DirectX 9, не менее 128 МБ видеопамяти; |
| **Привод DVD** | + | + |
| **Операционная cистема:** | Windows XP Home service pack 3 | Windows 7 профессиональная |
| **Дополнительные требования:** | Возможность вывода аудио сигнала;  Microsoft Windows Installer 2.0 или выше;  Доступ в Интернет;  Microsoft Internet Explorer 6.0 или выше;  свободный порт USB. | Возможность вывода аудио сигнала;  Microsoft Windows Installer 2.0 или выше;  Доступ в Интернет;  Microsoft Internet Explorer 8.0 или выше;  свободный порт USB. |

1. **Рекомендации по оптимизации затрат на создание СиЗИ ИСПДн**

В целях снижения затрат на создание СиЗИ ИСПДн. могут быть рекомендованы следующие способы:

1. **Обезличивание ПДн.**

**Обезличивание персональных данных** *–* действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных (ФЗ №152)

В соответствии с ФЗ №152 оператор наделен правом проводить обезличивание ПДн.

На момент подготовки настоящих Методических рекомендаций, в нормативно-правовой базе РФ в части защиты персональных данных, отсутствуют жесткие требования по реализации конкретных действий по обезличиванию ПДн.

Таким образом, методы и способы обезличивания ПДн. **оператор** **определяет самостоятельно**

|  |  |
| --- | --- |
| **Действия по обезличиванию ПДн.** | **Источник:** [**http://lukatsky.blogspot.com/2009/04/blog-post\_14.html**](http://lukatsky.blogspot.com/2009/04/blog-post_14.html) |
| * Абстрагирование ПДн – сделать их менее точными, например, путем группирования общих характеристик; * Скрытие ПДн – удалить всю или часть записи ПДн; * Внесение шума в ПДн – добавить небольшое количество посторонней информации в ПДн; * Замена ПДн – переставить поля одной записи ПДн с теми же самыми полями другой аналогичной записи; * Замена данных средним значением – заменить выбранные данные средним значением для группы ПДн; * Разделение ПДн на части – использование таблиц перекрестных ссылок; * Маскирование ПДн - замена одним символов в ПДн другими | |

1. **Cегментирование ИСПДн, ;**

**Сегментирование** — процесс разделения ИСПДн на взаимодействующие участки сети, который можно применять для оптимизации набора средств защиты информации, используемых в каждом сегменте. Это приводит, с одной стороны, к снижению стоимости защиты, а с другой — снижает избыточность СЗИ в тех случаях, когда защищаемые данные расположены неравномерно по сети.

**Из п. 2.4 приказа ФСТЭК России №58:** "При разделении информационной системы при помощи межсетевых экранов на отдельные части системы для указанных частей системы может устанавливаться более низкий класс, чем для информационной системы в целом".

Подробные сведения о методах и способах сегментирования ИСПДн. размещены в сети Интернет по адресу: [www.securitycode.ru/documents/upload/60](http://www.securitycode.ru/documents/upload/60)

1. **Инвентаризация и анализ, реализованных программно-аппаратных СЗИ.**

В процессе проведения внутренней проверки настоятельно рекомендуется, для каждой выявленной ИСПДн в организации, составить перечень реализованных программно-технических средств защиты информации ИСПДн (Наименование СЗИ, функциональное предназначение, реализация, версия, наличие лицензии на продукт, наличие сертификатов по требованиям безопасности)

Анализ данной информации может помочь оператору снизить затраты на внедрение СиЗИ ИСПДн.

Рассмотрим данный способ на примере подсистемы антивирусной защиты (рис.2.).

**рис.2.**

10. Заключение.

С учетом вышесказанного, оптимальным вариантом практической реализации технических мер по приведению ИСПДн., применяемых для обработки ПДн. при осуществлении нотариальной деятельности, в соответствие с требованиями ФЗ №152, следует считать комплексный подход приведенный на **схеме 3.**

|  |
| --- |
|  |